Proposed Draft Technical Report **ISO/IEC PDTR 15446**	
Date: **2000-01-04**	Reference number: ISO/IEC JTC 1/SC 27 **N 2449**
Supersedes document SC 27 N 2333	

THIS DOCUMENT IS STILL UNDER STUDY AND SUBJECT TO CHANGE. IT SHOULD NOT BE USED FOR REFERENCE PURPOSES.

ISO/IEC JTC 1/SC 27 Information technology - Security techniques Secretariat: Germany (DIN)	Circulated to P- and O-members, and to technical committees and organizations in liaison for voting (P-members only) by: **2000-04-03** Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.

ISO/IEC PDTR 15446

Title: Information technology – Security techniques – Guide for the production of protection profiles and security targets

Project: 1.27.22

Introductory note:
In accordance with resolution 7 (SC 27 N 2466) of the 11th SC 27 plenary meeting in Columbia, USA, October 1999, the attached document is hereby being submitted for a three-month PDTR letter ballot closing

April 3, 2000

Medium: Server

No. of pages. : 157

Address Reply to:

Secretariat, ISO/IEC JTC 1/SC 27 -
DIN Deutsches Institut fuer Normung e.V., Burggrafenstr. 6, 10772 Berlin , Germany
Telephone: + 49 2601-2652; Facsimile: + 49 2601-1723; E-Mail: passia@ni.din.de,
HTTP://www.din.de/ni/sc27

Vote on Proposed Draft Technical Report
ISO/IEC PDTR 15446

Date of circulation: **2000-01-04** Closing date: **2000-04-03**	Reference number ISO/IEC JTC 1/SC 27 **N 2449**

ISO/JTC 1/SC 27 Information technology – Security techniques Secretariat: Germany (DIN)	Circulated to P-members of the committee for voting Please return all votes and comments in electronic form directly to the SC 27 Secretariat by the due date indicated.
ISO/IEC PDTR 15446 Title: Information technology – Security techniques – Guide for the production of protection profiles and security targets Project: 1.27.22	

Vote:

_____	APPROVAL OF THE DRAFT AS PRESENTED
_____	APPROVAL OF THE DRAFT WITH COMMENTS AS GIVEN ON THE ATTACHED
___	general:
___	technical:
___	editorial:
_____	DISAPPROVAL OF THE DRAFT FOR REASONS ON THE ATTACHED
___	Acceptance of these reasons and appropriate changes in the text will change our vote to approval
_____	ABSTENTION (FOR REASONS BELOW):

P-member voting:

National Body (Acronym)

Date:

CCYY-MM-DD

Submitted by:

Name

Address Reply to:
Secretariat, ISO/IEC JTC 1/SC 27- DIN Deutsches Institut für Normung e.V., Burggrafenstr. 6, 10772 Berlin, Germany
Telephone: + 49 30 2601-2652; Facsimile: + 49 30 2601-1723; E-Mail: passia@ni.din.de; HTTP://www.din.de/ni/sc27

CONTENTS

1 Introduction

1.1 Objective and Intended Audience

This document provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with ISO/IEC 15408 (the 'Common Criteria'). This version is the eighth working draft of the guide. (1)

As such, the document is primarily aimed at those who are involved in the development of PPs and STs. However, it is also likely to be useful to evaluators of PPs and STs and to those who are responsible for defining and monitoring the application of the methodology for PP and ST evaluation. It may also be of interest to consumers and users of PPs and STs who wish to understand what guidance the PP/ST author used, and which parts of the PP or ST are of principal interest. (2)

It is assumed that readers of this Guide are familiar with Part 1 of ISO/IEC 15408 [15408-1], and in particular Annexes B and C which describe PPs and STs. PP and ST authors will (of course) need to become familiar with the other parts of ISO/IEC 15408 as described in this Guide, including introductory material such as the functional requirements paradigm described in [15408-2] subclause 1.3. (3)

1.2 Purpose and Scope of the Guide

This document is an informational ISO Technical Report provided for guidance only. This Guide should not be cited as an authority on the content or structure for the evaluation of PPs and STs. The Guide is intended to be fully consistent with ISO/IEC 15408; however, in the event of any inconsistency between the Guide and ISO/IEC 15408, the latter takes precedence. (4)

This Guide does not deal with issues such as PP registration and associated problems such as the handling of protected know-how (e.g. patents) in a PP. See [WD-15292] which proposes a definition of PP registration procedures. (5)

1.3 Protection Profiles and Security Targets - an Introduction

1.3.1 Purpose of a PP

The purpose of a PP is to state a security problem rigorously for a given set or collection of systems or products - known as the Target Of Evaluation (TOE) - and to specify security requirements to address that problem without dictating how these requirements will be implemented. (For this reason, a PP is said to provide an implementation-independent security description.) A PP thus includes several related kinds of security information: (6)

a) A PP overview and a TOE description which identify, in terms appropriate for users of information technology, the statement of need or security problem to be addressed.

b) A description of the TOE security environment which refines the statement of need with respect to the intended environment of use, producing the threats to be countered and the organisational security policies to be met in light of specific assumptions.

c) Security objectives which scope the TOE evaluation based on the description of the TOE security environment, giving information about how, and to what extent, the security needs are to be met. The purpose of a security objective is to mitigate risk and to support the security policies of the PP sponsor.

d) Security functional requirements and assurance requirements which address the problem posed by the statement of need, to the extent defined by the security objectives for the TOE and its IT environment. The security functional requirements explain what must be done by the TOE, and what must be done by its IT environment, in order to meet the security objectives. The assurance requirements explain the degree of confidence expected in the security functions of the TOE.

e) A rationale which demonstrates that the security functional requirements and assurance requirements suffice to meet the statement of need. The security objectives must explain what is to be done about the security concerns found in the description of the TOE security environment. The security functional requirements and assurance requirements must meet the security objectives.

1.3.2 Purpose of an ST

An ST is similar to PP, except that it contains additional implementation-specific information detailing how the security requirements are realised in a particular product or system. Thus, the ST contains the following additional information not found in a PP: (7)

a) A TOE summary specification that presents TOE-specific security functions and assurance measures.

b) An optional PP claims portion that explains which PPs the ST is claimed to be conformant with, if any.

c) Finally, the rationale contains additional evidence establishing that the TOE summary specification ensures satisfaction of the implementation-independent requirements, and that any claims about PP conformance are satisfied.

1.3.3 Usage of the PP and ST

A PP may be used to define a ‘standard’ set of security requirements with which one or more products may claim compliance, or which systems used for a particular purpose within an organisation must comply. (See [15408-1] subclause 2.3 for the definition of the terms *product* and *system*, and also [15408-1] subclause 4.1.2 for a general discussion of the distinction between the two). A PP may apply to a particular type of TOE (e.g. operating system, database management system, smartcard, firewall, and so on), or it could apply to a set of products grouped together in a *composite* TOE (system or product). (8)

Product vendors may respond to the security needs defined by a PP by producing an ST which demonstrates how their product addresses those security needs. However, it is not mandatory for an ST to claim conformance with a PP; for example, an ST may be written to specify the security functions claimed by a product vendor, thereby forming the baseline for the product evaluation.(9)

A PP may also define the security requirements to be satisfied by a specific IT system. In this event, the ST is proposed in response to the PP, i.e. the ST may be written in response to an RFP (Request For Proposal) or ITT (Invitation To Tender) that references the PP. A PP and ST can thus be used as a means of communication among the party responsible for managing the development of a system, the stakeholders in that system, and the organisation responsible for producing the system (hereafter referred to as the developer). The content of the PP and ST may be negotiated among the players. Evaluation of the actual system against the ST - which has been confirmed as conformant with the PP - may be part of the acceptance process. (It should of course be noted that an ST may be written by a developer as part of a response to an RFP or ITT that does not reference a PP.) (10)

1.4 Overview of the Guide

This Guide provides detailed guidance relating to the various parts of a PP or ST, and how they interrelate. For a summary of the key points of guidance contained in this document, presented in the form of a checklist, the interested reader should consult Annex A. (11)

This Guide is structured such that the guidance to PP and ST authors is presented in the main body of the Guide (i.e. the individual Chapters), with a summary presented in Annex A as mentioned above. Subsequent annexes then present a variety of examples to illustrate application of the guidance. (12)

Chapter 2 provides an overview of the PP and ST which presents example contents lists and highlights the expected contents of, and the target audience for, the various parts of a PP or ST. This chapter also discusses the relationship between the PP and the ST and issues relating to the PP/ST development process. Chapter 3 examines in more depth the descriptive parts of a PP and ST, covering the PP and ST introduction and the TOE description (which tend to be more aimed at consumers and users) as well as PP application notes (which tend to be more aimed at ST authors and TOE developers). (13)

The next five chapters of the Guide follow the order of the PP and ST contents as outlined in ISO/IEC 15408 ([15408-1] Figures B.1 and C.1). (14)

Chapter 4 gives guidance on the definition of the TOE security environment in a PP or ST, which covers the various aspects of the ‘security needs’ to be met by the TOE. Chapter 5 then provides guidance on the definition of the intended response to the different aspects of the security needs by the TOE and its environment, as given in the specification of security objectives in a PP or ST. Both of these chapters are of general interest, not only to PP/ST authors, but also to others such as consumers and users of PPs and STs. (15)

Chapter 6 provides guidance on the selection and specification of IT security requirements in a PP. This chapter goes into some detail describing how the functional and assurance components defined in ISO/IEC 15408, as well as non-ISO/IEC 15408 components, should be used to provide a clear definition of the IT security requirements. Chapter 7 then provides specific guidance relating to STs, covering the specification of IT security requirements (and how this differs from the PP case) and the TOE summary specification. As such, these two chapters will be mainly of interest to PP/ST authors and evaluators. (16)

Chapters 8 and 9 provide guidance on the construction and presentation of the Rationale sections of a PP and ST. Such guidance is likely to be of prime interest to PP/ST authors and evaluators. The approach taken is first (in Chapter 8) to describe the construction of the PP Rationale. Then (in Chapter 9), the Guide moves on to consider the ST Rationale, providing guidance on those aspects which differ from the PP Rationale. (17)

Chapter 10 examines the issues specific to PPs and STs for *composite TOEs*, i.e. TOEs that are composed of two or more *component TOEs*, each of which has its own PP or ST. (18)

Chapter 11 provides guidance on the construction of functional and assurance packages, which are defined so as to be useable in different PPs and STs. A package is thus seen as potentially a very useful tool intended to promote and facilitate cost-effective construction of PPs and ST. (19)

As described above, Annex A summarises the guidance in the form of a checklist. (20)

Annex B presents example threats, organisational security policies, assumptions, and security objectives, and identifies appropriate ISO/IEC 15408 Part 2 functional components for specifying common or generic security functional requirements. Although these examples are intended to be wide-ranging, they are in no way claimed to be exhaustive. (21)

Annex C provides guidance that specifically relates to PPs and STs for TOEs which implement cryptographic functionality. Such guidance has been included to cover a wide range of such TOEs, and deal with the specific issues relating to specification of cryptographic functionality. (Future versions of the Guide may include similar annexes for other types of TOE.) (22)

Annexes D to F illustrate application of the guidance in a variety of contexts, using worked examples for different types of TOE. Each of these examples is based on actual PPs and STs that have been developed (independent of this Guide). In Annex D, we see application of guidance to the construction of a firewall PP and ST. Annex E discusses a database management system PP, where it can be seen that the issue of dependencies on the IT environment is of particular importance. Finally, Annex F examines the issues surrounding the development of a Trusted Third Party (TTP) PP. (23)

1.5 Glossary

Terminology used in this Guide is as defined in subclause 2.3 of [15408-1] unless otherwise specified. (24)

The following abbreviations are used in this Guide in addition to the abbreviations listed in subclause 2.1 of [15408-1]: (25)

DBMS	Database Management System
ITT	Invitation to Tender
OSP	Organisational Security Policy
RFP	Request for Proposal
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
TSS	TOE Summary Specification
TTP	Trusted Third Party

1.6 References

[15408-1] Evaluation Criteria for IT Security
Part 1: Introduction and general model
ISO/IEC 15408-1: 1999(E), December 1998

[15408-2] Evaluation Criteria for IT Security
Part 2: Security functional requirements
ISO/IEC 15408-2: 1999(E), December 1998

[15408-3] Evaluation Criteria for IT Security
Part 3: Security assurance requirements
ISO/IEC 15408-3: 1999(E), December 1998

[GMITS] Guidelines for the Management of IT Security (GMITS)
Part 1: Concepts and models of IT Security
Part 2: Managing and planning IT Security
Part 3: Techniques for the management of IT Security
Part 4: Selection of Safeguards
Part 5: Safeguards for external connection

[ISO-2382] Information Technology - Vocabulary
Part 8: Security (Revision of ISO 2382-9:1986)
ISO/IEC DIS 2382-8, Edition 2.

[WD-15292] Information Technology - Security techniques -
Protection Profile registration procedures
ISO/IEC WD 15292, 1999-06-11

Editor note: other applicable standards will be referenced as and when they are identified.

2 Overview Of The PP And ST

2.1 Introduction

This chapter provides an overview of the PP and ST, summarising the contents of both documents, discussing the relationship between the PP and ST, and the process by which the documents are developed. See also [15408-1] Annexes B and C. (26)

2.2 The Protection Profile

The required content of a PP is portrayed in [15408-1] Annex B, Figure B.1, page 38. Table 1 below translates this into an example contents list. (27)

1	PP INTRODUCTION 1.1 PP Identification 1.2 PP Overview
2	TOE DESCRIPTION
3	TOE SECURITY ENVIRONMENT 3.1 Assumptions 3.2 Threats 3.3 Organisational Security Policies
4	SECURITY OBJECTIVES 4.1 Security Objectives for the TOE 4.2 Security Objectives for the Environment
5	IT SECURITY REQUIREMENTS 5.1 TOE Security Functional Requirements 5.2 TOE Security Assurance Requirements 5.3 Security Requirements for the IT Environment
6	PP APPLICATION NOTES
7	RATIONALE 7.1 Security Objectives Rationale 7.2 Security Requirements Rationale

Table 1 - Example Protection Profile Contents List

The *PP Introduction* identifies the PP and provides a summary of the PP in narrative form, suitable for inclusion in PP catalogues and registers. This section is discussed in more detail in Chapter 3 of this Guide. (28)

The *TOE Description* provides background information to the TOE (or TOE type), and serves as an aid to the understanding of its security requirements and intended usage. This section is discussed in more detail in Chapter 3 of this Guide. (29)

The *TOE Security Environment* provides a definition of the context in which the TOE resides, and in particular defines the ‘security needs’ the TOE is intended to address. This description details any assumptions defining the scope of the security needs, the identified threats to the assets requiring protection (together with a description of those assets), and any organisational security policies with which the TOE must comply. This section is discussed in detail in Chapter 4 of this Guide. (30)

The *Security Objectives* provide a concise statement of the intended response to the security needs, both in terms of the security objectives to be satisfied by the TOE, and the security objectives to be satisfied by IT and non-IT measures within the TOE environment. This section is discussed in detail in Chapter 5 of this Guide. (31)

The *IT Security Requirements* define the security functional requirements on the TOE, the security assurance requirements, and any security requirements on software, firmware and/or hardware in the IT environment for the TOE. The IT security requirements are to be defined using, where applicable, functional and assurance components from ISO/IEC 15408 Part 2 [15408-2] and Part 3 [15408-3]. This section is discussed in detail in Chapter 6 of this Guide. (32)

The *PP Application Notes* is an optional section providing any additional supporting information considered useful by the PP author. Note that application notes may be distributed amongst the relevant sections of the PP instead of being provided in a separate section. This is discussed in more detail in Chapter 3 of this Guide. (33)

The *Rationale* provides a demonstration that the PP specifies a complete and cohesive set of IT security requirements, and that a conformant TOE would effectively address the defined security needs. This is discussed in detail in Chapter 8 of this Guide. (34)

Note that there are a number of optional sections or more detailed sub-sections that should also be considered for inclusion. Note also that the Rationale section may be packaged as a separate document, as stated in [15408-1], subclause B.2.8, page 42. (35)

In practice, additional sections may be necessary to provide useful information to the reader, for example: (36)

a) the *PP Introduction* section might include a subsection describing the organisation of the PP, and provide references to related PPs and other relevant documents;

b) the *TOE Security Environment* section might include separate subsections for various domains in the TOE IT environment;

c) the *IT Security Requirements* section might be extended to include detail on security requirements for the non-IT environment where the PP author considers them useful.

Where identified sections are not applicable (e.g. organisational security policies, IT security requirements for the environment) these should be replaced by an appropriate statement to that effect. (37)

2.3 The Security Target

The required content of an ST is portrayed in [15408-1] Annex C, Figure C.1, page 44. Table 2 below translates this into an example contents list. (38)

1	ST INTRODUCTION 1.1 ST Identification 1.2 ST Overview 1.3 ISO/IEC 15408 Conformance
2	TOE DESCRIPTION
3	TOE SECURITY ENVIRONMENT 3.1 Assumptions 3.2 Threats 3.3 Organisational Security Policies
4	SECURITY OBJECTIVES 4.1 Security Objectives for the TOE 4.2 Security Objectives for the Environment
5	IT SECURITY REQUIREMENTS 5.1 TOE Security Functional Requirements 5.2 TOE Security Assurance Requirements 5.3 Security Requirements for the IT Environment
6	TOE SUMMARY SPECIFICATION 6.1 TOE Security Functions 6.2 Assurance Measures
7	PP CLAIMS 7.1 PP Reference 7.2 PP Refinements 7.3 PP Additions
8	RATIONALE 8.1 Security Objectives Rationale 8.2 Security Requirements Rationale 8.3 TOE Summary Specification Rationale 8.4 PP Claims Rationale

Table 2 - Example Contents List for a Security Target

The *ST Introduction* identifies the ST and TOE (including its version number) and provides a summary of the ST in narrative form, suitable for inclusion in evaluated products lists. This section is discussed in more detail in Chapter 3 of this Guide. (39)

The *TOE Description* provides background information to the TOE, and serves as an aid to the understanding of its security requirements and intended usage. The TOE description should also include a definition of the configuration in which the TOE is to be evaluated. This section is discussed in more detail in Chapter 3 of this Guide. (40)

The *TOE Security Environment* provides a definition of the context in which the TOE resides, and in particular defines the ‘security needs’ the TOE is intended to address. This description details any assumptions defining the scope of the security needs, the identified threats to the assets requiring protection (together with a description of those assets), and any organisational security policies with which the TOE must comply. This section is discussed in detail in Chapter 4 of this Guide. (41)

The *Security Objectives* provide a concise statement of the intended response to the security needs, both in terms of the security objectives to be satisfied by the TOE, and the security objectives to be satisfied by IT and non-IT measures within the TOE environment. This section is discussed in detail in Chapter 5 of this Guide. (42)

The *IT Security Requirements* define the security functional requirements on the TOE, the security assurance requirements, and any security requirements on software, firmware and/or hardware in the IT environment for the TOE. The IT security requirements are to be defined using, where applicable, functional and assurance components from ISO/IEC 15408 Part 2 [15408-2] and Part 3 [15408-3]. This section is discussed in detail in Chapter 6 of this Guide. (43)

The *TOE Summary Specification* defines the IT security functions provided by the TOE to meet the specified security functional requirements, and also any assurance measures claimed to satisfy the specified security assurance requirements. This is discussed in detail in Chapter 7 of this Guide. (44)

The *PP Claims* is an optional section which identifies any PPs with which the ST is claimed to conform, and any additions or refinements of the PP objectives or requirements. This is discussed in detail in Chapter 9 of this Guide. (45)

The *Rationale* provides a demonstration that the ST specifies a complete and cohesive set of IT security requirements, that a conformant TOE would effectively address the defined security needs, and that the IT security functions and assurance measures are suitable to meet the TOE security requirements. This is discussed in detail in Chapter 9 of this Guide. (46)

As with the example contents list for a PP (see section 2.2 above), in practice an ST author may profitably depart from the above structure by including additional sections or subsections, or by omitting optional (not applicable) sections. (47)

2.4 Relationship between the PP and ST

It will be evident from comparison of the example contents list in Tables 1 and 2 that there is a high degree of commonality between a PP and an ST, in particular within the *TOE Security Environment*, *Security Objectives* and *IT Security Requirements* sections, and the parts of the *Rationale* section which address these aspects. Indeed, if an ST simply claims conformance with a PP with no additional functional or assurance requirements, then the content of these sections of the ST may be identical to that the corresponding sections in the PP. In such cases it is recommended that the ST simply references the PP content, providing detail only where it differs from the PP. (48)

The following sections in the ST provide detail that will not be featured in a PP, reflecting the specific nature of the ST, i.e. as a definition of how the TOE will provide a solution to the defined security needs: (49)

a) the *TOE Summary Specification*, covering IT security functions, security mechanisms or techniques, and assurance measures;

b) the optional *PP Claims*, detailing and justifying any claims of compliance with referenced PP(s);

c) those parts of the *Rationale* in the ST which demonstrate the adequacy of the IT security functions and the assurance measures to satisfy the TOE security requirements.

2.5 Aiming a PP or ST at its Target Audience

One of the key challenges in writing a PP or ST is to factor the presentation so that all of the intended audiences are properly served: (50)

a) Consumers (i.e. procurers and high-level decision-makers) need a general understanding of what conforming TOEs will provide in the way of security. For successful PPs, this may be the largest class of readers.

b) Developers (including implementers in the case of an ST) need an unambiguous definition of security requirements in order to build conforming TOEs.

c) TOE users (including installers, administrators, and maintainers) need information on the required TOE security environment.

d) Evaluators need information that will justify the technical soundness and effectiveness of the PP or ST.

PPs and STs are designed in such a way that different sections serve different audiences, and they need to be written accordingly. (51)

The *PP/ST Introduction*, *TOE Description*, and *TOE Security Environment* sections should be written primarily for consumers. The *Security Objectives* section may be also written for consumers. It should, however, be remembered that TOE developers will also need to take account of information in the *TOE Security Environment* and *Security Objectives* sections. (52)

The *IT Security Requirements* section of the PP should be written primarily for TOE developers, although the information it contains is also likely to be of interest to TOE consumers. Conversely, the *TOE Summary Specification* section of a ST should be written primarily for evaluators and consumers. If these sections are not self contained, they should explicitly indicate which other PP sections (e.g. the PP Glossary) and which other documents (e.g. referenced encryption standards) are necessary for a full and accurate understanding of the presented IT security requirements. In particular, if the *TOE Summary Specification* depends for its meaning on the *IT Security Requirements* section, this fact should be explicitly pointed out. (53)

Evaluators need to be familiar with all sections of a PP or ST. However, information intended primarily for evaluators should be presented in the *Rationale* section. (54)

2.6 The PP and ST Development Process

The presentation of the requirements for PPs and STs in [15408-1] annexes B and C, and in [15408-3] clauses 3 to 5, might suggest that it is expected that PPs and STs are always developed in a logical 'top-down' manner, e.g. (in the case of a PP) that: (55)

a) the security needs are first defined;

b) the security objectives are then identified to address those needs;

c) IT security requirements are then defined to satisfy the security objectives for the TOE.

Whilst such a possibility is not ruled out, it is more likely that an iterative process will be required. For example, definition of IT security requirements may highlight clarifications needed to the definition of the security objectives, or even the security needs. In general, a number of iterations may be required in which the relationships between threats, organisational security policies, security objectives and IT security requirements and functions are examined closely, particularly when the PP or ST Rationale is being constructed. Only when all identified gaps in the rationale are filled may it be assumed that the PP or ST is complete. (56)

The PP or ST development process may also need to accommodate changes to the document in order to reflect changes in external circumstances, for example: (57)

a) new threats may be identified;

b) organisational security policies may change;

c) cost and time constraints may impose changes in division of responsibility between what the TOE is expected to do, and what is expected of the TOE environment;

d) changes in technology and development costs may impact on IT security requirements, security functions or assurance measures.

It is also possible (e.g. if the TOE is a product which has already been developed) that the PP or ST author already has a clear idea of the SFRs that the TOE will meet (even if these have not yet been expressed in the way ISO/IEC 15408 requires). In such cases the definition of the security needs and security objectives will unavoidably be influenced by the knowledge of the form of the security solution the TOE provides. The PP/ST development process will in those cases be, to some extent, 'bottom-up'. (58)

2.7 PP Families

A 'PP family' is (as its name suggests) a set of closely related PPs, which typically apply to the same product or system type (e.g. operating system, firewall, and so on). A PP may thus be developed as part of a wider process of developing a family of PPs. Possibilities include the development of: (59)

a) a series of hierarchically related PPs for the same type of TOE (one PP may be said to be hierarchic to another PP in the family if it includes all IT security requirements specified in the other PP);

b) a set of PPs that apply to different components of an IT system, e.g. a smartcard family might include PPs for the integrated circuit card, operating system, application, smartcard reader, and so on.

Where a PP family applies to a particular type of TOE, it is important that there is a clear distinction between different members of the family. In other words, there should be clear differences in the TOE security requirements; and it follows from this that the PPs should at least differ in their security objectives (which drive the selection of IT security requirements), if not the statement of TOE security environment. For example, consider the case where two PPs specify the same set of SFRs, but a different set of SARs. It may be possible to justify a lower assurance requirement by an increase in the environmental security. Such differences should be reflected in the security objectives. (60)

Where a family of PPs applies to different components of an IT system (whether in a specific or assumed environment), the relationship between the PPs should be made clear. See also Chapter 10 of this Guide, which discusses issues relating to definition of PPs for components of an IT system. (61)

3 Descriptive Parts of the PP and ST

3.1 Introduction

This chapter provides guidance on the construction of the purely descriptive parts of a PP and ST, namely: (62)

a) the PP and ST Introduction;

b) the TOE Description in a PP or ST;

c) PP application notes.

3.2 Descriptive parts of the PP

3.2.1 PP Introduction

PP Identification

The intent of this section ([15408-1], subclause B.2.2a) is to provide sufficient identification information to uniquely identify the PP, possibly for the purposes of registration of the PP. As a minimum this will include the PP name and a identifier that is unique to that version of the PP. The following information may also be useful (or may be required by a PP registry): (63)

a) key words;

b) EAL (if applicable);

c) CC conformance claim and ISO/IEC 15408 version;

d) PP evaluation status.

ISO/IEC 15408 does not dictate where in the *PP Introduction* the EAL (if any) should be included, but it is recommended that the EAL be placed here, as it plays a prominent role in international mutual recognition. (64)

The CC conformance claim should also be placed in the introduction for the same reasons, as enumerated in [15408-1], subclause 5.4, page 31. (65)

The ISO/IEC 15408 version needs to be included for reasons of version control, although ISO/IEC 15408 does not explicitly call for it. This should be evident in the *Referenced Documents* section (see below), but it may be useful to highlight the version in the *PP Identification*. (66)

PP Overview

According to ISO/IEC 15408, the *PP Overview* should be a summary of the PP in narrative form, usable as a stand-alone abstract for use in PP catalogues and registers. A top-level overview of the security problem being solved with the PP should be included but is not explicitly required. A top-level overview of how the PP contributes to the solution is also advisable. You should of course ensure that this overview is consistent with the technical content of the PP. (67)

In the likely case that the intended consumer audience for the PP includes high-level decision-makers, the *PP Overview* may be expanded to an Executive or Management Summary. However, if it is intended that the PP is included in a PP registry, you should ensure that an appropriate abstract of the PP (typically one or two paragraphs) can be readily extracted from the *PP Overview* for entry in the registry. (68)

Related PPs and Referenced Documents (Optional)

Wherever a PP is known, or is intended to have, a close relationship to one or more other existing PPs, it is recommended that these related PPs are identified in the *PP Introduction* section. It will also be helpful to the reader if the nature of the relationship is highlighted. (Note that evaluation of a PP which has a close relationship to an existing PP may be able to make use of the evaluation results for that PP, and thus focus on the differences between the two.) It should, however, be stressed that the intent here is simply to provide information that will be useful to the reader, and which is already known to the PP author; there is no need for the PP author to undertake any detailed survey of existing PPs.

A PP for a large distributed system will naturally incorporate several other documents by reference (e.g. previous threat studies, high-level summary documents bearing on the TOE description, and documents describing various components of the IT environment). Such documents may have been developed over a span of years and written by multiple organisations. They may well represent inconsistencies with regard to terminology, viewpoint, environment, and security objectives. In such cases, it is important for the PP to carefully explain what is and is not being taken from documents that are being incorporated by reference. (69)

PP Organisation (Optional)

Readers not familiar with typical PP structure will need an explanation of its structure and organisation. This explanation of structure is traditionally presented in a document's introduction. The following boilerplate may be inserted if appropriate (italicised text in square brackets is used to indicate where the boilerplate text is dependent on the PP/ST content and structure): (70)

> The main sections of the PP are the TOE description, TOE Security Environment, Security Objectives, IT Security Requirements, and Rationale. [*If the PP includes security requirements for the non-IT environment, then the IT Security Requirements section is more accurately identified as just "Security Requirements."*]
>
> The TOE description provides general information about the TOE, serves as an aid to understanding its security requirements, and provides context for the PP's evaluation.
>
> The TOE security environment describes security aspects of the environment in which the TOE is to be used and the manner in which it is to be employed. [*If there are distinct domains for the TOE environment, optionally include the following text: "The security environmental aspects are discussed separately for distinct domains of the TOE security environment"*.] The TOE security environment includes descriptions of a) assumptions regarding the TOE's intended usage and environment of use, b) threats relevant to secure TOE operation, and c) organisational security policies with which the TOE must comply [*omit item b) or c) if appropriate*].
>
> The security objectives reflect the stated intent of the PP. They pertain to how the TOE will counter identified threats and how it will cover identified organisational

security policies and assumptions. Each security objective is categorised as being for the TOE or for the environment [*include if appropriate: "or both"*].

[*The first sentence to be included on Security Requirements should be selected according to which of the options permitted by ISO/IEC 15408 are chosen by the PP/ ST author:*

- *Option 1, TOE Security Requirements only:*
  "All of the requirements in this PP apply to the TOE itself, as opposed to the TOE environment."
- *Option 2, TOE and IT environment only:*
  "The IT Security Requirements section provides detailed security requirements, in separate subsections, for the TOE and its environment."
- *Option 3, TOE and environment, including the non-IT environment:*
  "The Security Requirements section provides detailed security requirements, in separate subsections, for the TOE and its environment."]

The IT security requirements are subdivided as follows: (a) TOE Security Functional Requirements [*if AVA_SOF.1 is included in the assurance requirements, add the following text: "including strength of function requirements for TOE security functions realised by a probabilistic or permutational mechanism"*], and (b) TOE security assurance requirements.

The Rationale presents evidence that the PP is a complete and cohesive set of IT security requirements and that a conformant TOE would effectively address the security needs.

The Rationale is factored into two main parts. First, a Security Objectives Rationale demonstrates that the stated security objectives are traceable to all of the aspects identified in the TOE security environment and are suitable to cover them. Then, a Security Requirements Rationale demonstrates that the security requirements (TOE and environment) are traceable to the security objectives and are suitable to meet them.

3.2.2 TOE Description

The TOE Description should contain the following kinds of information (the first two are mandated by ISO/IEC 15408, the latter two are suggested): (71)

a) product type;

b) general TOE functionality;

c) TOE boundary (optional);

d) TOE operational environment (optional).

The general TOE functional description is just that. It is not simply a description of TOE security features, unless the TOE is a special-purpose security product. (72)

The optional description of the TOE boundary tells the reader what is in the TOE and what is not. It is possible for the PP to provide some flexibility between environment and TOE in compliant STs. However, the range of allowable choices should be bounded and explicit. (73)

The optional description of the operational environment tells the reader where the TOE is used, covering important assumptions, business process constraints, and other key elements that are of most concern to higher-level PP users. (74)

You should ensure that the TOE description does not present an inaccurate or misleading picture of the intended usage of the TOE or its security functionality, e.g. describes security features or configurations that are not within the scope of the intended evaluation of the TOE. (75)

3.2.3 Application notes

Application Notes are optional in a PP, and may either be included in a separate section, or they may be interspersed throughout the document, for example to accompany individual TOE security requirements. Application notes should be used to provide any supporting information that you consider relevant or useful for the construction, evaluation, or use of the TOE. A typical use of application notes is to provide clarifications of how particular security requirements are to be interpreted in the context of the TOE, or to provide advice to ST authors as to how operations on functional components might be completed in the ST. (76)

If the application notes are integrated into text throughout the PP, it is recommended that individual application notes are clearly identified as such, so that the reader clearly understands that the text is informative and is not, for example, a refinement of an SFR or SAR. (77)

3.3 Descriptive parts of the ST

3.3.1 ST Introduction

The guidance relating to the construction of the PP introduction is applicable, with the following exceptions: (78)

a) the CC conformance claim is not optional in an ST;

b) PP registration procedures do not apply;

c) an identification of related STs may be appropriate if the TOE is a composite TOE, or is part of a composite TOE.

3.3.2 TOE Description

The guidance relating to the provision of the TOE description for a PP is applicable, with the exception that the definition of the TOE boundary must be provided, both in a physical way (hardware and/or software components/modules) and in a logical way (IT and security features offered by the TOE). (79)

4 The TOE Security Environment

4.1 Introduction

This chapter provides guidance on the specification of the *TOE Security Environment* section of a PP or ST. ISO/IEC 15408 defines the requirements for the content of this part of a PP or ST in [15408-1], subclauses B.2.4 and C.2.4. The wording of these two sections is identical, which can be taken as an indication that the expected content of the *TOE Security Environment* section does not differ greatly between a PP and an ST. (80)

The purpose of the *TOE Security Environment* section is to define the nature and scope of the 'security needs' to be addressed by the TOE. This is illustrated in Figure 1 below. (81)

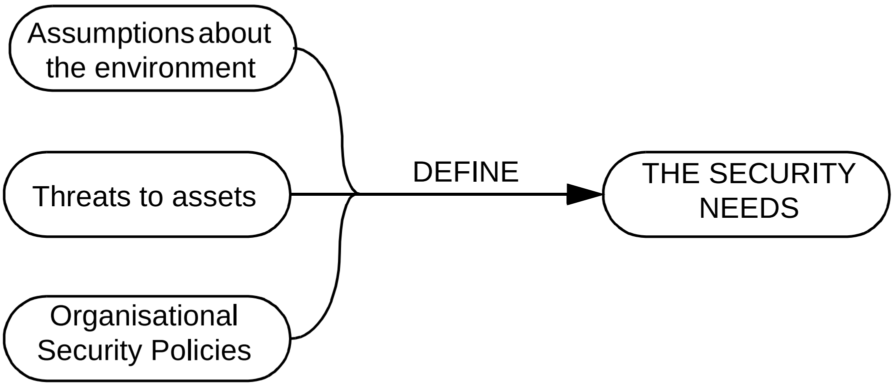
Assumptions about the environment
Threats to assets
Organisational Security Policies
DEFINE
THE SECURITY NEEDS

Figure 1 - Definition of the Security Needs

This section will therefore involve a discussion of: (82)

a) any assumptions that are made regarding the TOE security environment, thereby defining the scope of the security needs;

b) the assets requiring protection (typically information or resources within the IT environment or the TOE itself), the identified threat agents, and the threats they pose to the assets;

c) any organisational security policies or rules with which the TOE must comply in addressing the security needs.

Subsequent sections of the PP and ST show how the security needs will be addressed by the TOE, in combination with its operating environment. It is therefore important to ensure that the security needs are clearly and concisely defined - otherwise you may end up with a PP and ST that addresses the wrong needs. (83)

As a general principle, the definition of the security needs should avoid, where possible, any discussion of the form of the TOE's response to meeting the security needs, e.g. details relating to the TOE security functions. By following this principle, you will help to focus the reader's attention on what are the important aspects of the security needs. Discussion of how the security needs are to be satisfied by the TOE should be left to the later parts of the PP or ST. (84)

4.2 How to Identify and Specify the Assumptions

ISO/IEC 15408 requires the *TOE Security Environment* section of a PP or ST to contain a list of assumptions about the TOE security environment or the intended usage of the TOE. To compile such a list, you first need to ask the following question: (85)

> *What assumptions am I making about the TOE security environment and the scope of the security needs?*

For example, it may be necessary to make some assumptions in order to ensure that a potential threat to an asset is not, in practice, relevant in the TOE security environment. (86)

The following types of assumption should be included: (87)

a) aspects relating to the intended usage of the TOE;

b) environmental (e.g. physical) protection of any part of the TOE;

c) connectivity aspects (e.g. a firewall being configured as the only network connection between a private network and a hostile network);

d) personnel aspects (e.g. the types of user roles anticipated, their general responsibilities, and the degree of trust assumed to be placed in those users).

Other assumptions may be included where these have had a material effect on the PP or ST content, for example assumptions which led to the choice of the assurance requirement. However, it must be remembered that ISO/IEC 15408 requires that the formally identified assumptions have to be shown to be upheld by the security objectives. General assumptions which cannot be traced to security objectives may nonetheless be usefully included within the descriptive (informative) text in the PP or ST. (88)

It is unlikely that you will be able to completely identify all the assumptions you are making in a single attempt. Rather, you should expect to be identifying additional assumptions throughout the development of the PP or ST. In particular, when constructing the PP or ST rationale (e.g. demonstrating that the security objectives are suitable to counter the identified threats), you should consider whether you are making any assumptions that have not been stated in the PP or ST. (89)

When adopting this iterative approach to identifying assumptions, it is important (in line with the general principle stated above) to avoid the inclusion of any ‘assumptions’ relating to the effective use of specific TOE security functions that you identify in the process of constructing the rationale. Such detail would be more appropriately included as security requirements for the non-IT environment (see section 6.5.2). It is, however, reasonable to state as a ‘personnel’ assumption that (for example) the TOE has one or more administrators who are assigned responsibility for ensuring the TOE security functions are configured and used appropriately. (90)

For ease of reference, it is recommended that each assumption is numbered or otherwise uniquely labelled. (91)

Example assumptions are presented in Annex B of this guide. (92)

4.3 How to Identify and Specify the Threats

ISO/IEC 15408 requires that the PP or ST contains a description of *any threats to the assets against which protection will be required* ([15408-1], subclause B.2.4, page 39). However, ISO/IEC 15408 goes on to say that the statement of threats may be omitted if the security objectives are derived solely from the organisational security policies (OSPs): in other words, where the ‘security needs’ are defined in full by the OSPs and assumptions. This might be the case, for example, where an ST is being written in response to an RFP or ITT which defines those OSPs. (93)

In practice, it is recommended that a statement of threats be included in the PP or ST as these generally provide a better understanding of the security needs than a corresponding set of OSPs. Moreover, there is a danger in relying on the OSPs alone, since they may not be up-to-date and accurately reflect the current threat. If you already have a comprehensive set of OSPs you are nonetheless encouraged to extrapolate the threats that they address in order to facilitate maximum reuse of the PP, as well as to convey a more thorough understanding of the security needs. (94)

The importance of risk analysis should not be underestimated, since if it is not done properly the TOE may provide inadequate protection, as a result of which the organisation’s assets may be exposed to an unacceptable level of risk. It should, however, be noted that ISO/IEC 15408 does not provide a framework for risk analysis or the specification of threats at an organisational level. Similarly, a detailed discussion of the process by which the threats to the assets are identified (which is one of the hardest parts of an organisation’s risk analysis) is outside the scope of this Guide. However, for completeness, the general principles involved are stated below; see also [15408-1] clause 4. The reader is referred to standards such as [GMITS] for more detailed guidance on this topic. (95)

4.3.1 How should threats be identified?

A ‘threat’ (as described in [15408-1], subclause 4.1.1, page 13) is simply an undesirable event, which is characterised in terms of *a threat agent, a presumed attack method, any vulnerabilities that are the foundation for the attack, and identification of the asset under attack* ([15408-1], subclause 4.3.1, page 21). (Note that violations of the organisation’s security policy should not be treated as threats.) (96)

In order to identify what the threats are, you therefore need to answer the following questions: (97)

a) what are the assets that require protection?

b) who or what are the threat agents?

c) what attack methods or undesirable events do the assets need to be protected from?

Identifying the assets

ISO/IEC 15408 defines *assets* as *information or resources to be protected by the countermeasures of a TOE* ([15408-1], subclause 2.3, page 4). They are so named because they have some intrinsic value to those who own those assets (whether individuals or organisations). By the same token, they are often of value to threat agents who may seek to compromise the assets of those assets, contrary to the wishes and interests of the owner, for example by causing loss of confidentiality, integrity or availability of the assets. (98)

The *assets* of concern to the PP or ST author may be a representation of the primary assets of the organisation (e.g. monetary value, or an organisation’s personnel, customers, or reputation). In the context of the description provided in [15408-1] subclause 4.1.1, the *owners* of the assets should be understood as referring to those who are responsible for safeguarding the assets within the IT system (in which the TOE is deployed). In practice, the primary assets they represent may have multiple owners who differ from the owner of the TOE and of the information that the TOE contains. It may be helpful to the reader of a PP or ST to identify such primary owners when describing the assets. For example: (99)

a) in a Trusted Third Party (TTP), different keys will have different owners, i.e. TTP subscribers as well as the owner of the TTP itself (see the worked example in Annex F);

b) in the case of medical systems, it is commonly held that the TOE's information has no single owner, but rather consists of all those having an interest, due to the complex rules and considerations guiding its use and control.

ISO/IEC 15408 indicates that assets typically take the form of information which is stored, processed and transmitted by IT systems ([15408-1], subclause 4.1.2, page 15). It should be emphasised that the assets may be *external* to the TOE (but within the IT environment), as is the case with information and resources protected by firewalls or intrusion detection systems. (100)

ISO/IEC 15408 suggests that the identified assets may also include such things as authorisation credentials and the IT implementation, which are indirectly subject to security requirements ([15408-1], subclause 4.3.1, page 21). Such 'assets' might be identified as part of the process of identifying the countermeasures needed to protect the primary assets (or their representation). Although permitted by ISO/IEC 15408, it is not (in general) recommended that you identify explicitly as assets information and resources that introduced by the presence of the TOE itself, and which are only indirectly related to the primary assets. This is because the inclusion of such detail may: (101)

a) obscure the primary purpose of the TOE (which is to protect the primary assets or their representation within the IT environment);

b) lead to the introduction of implementation detail (i.e. the solution to the defined security needs) at too early a stage in the PP or ST, which will then be promulgated through to the threats and security objectives.

Identifying the threat agents

As described above, *threat agents* may either be human or non-human, although (as pointed out by [15408-1], subclause 4.1.1, page 13) in the domain of security greater attention is usually given to those threats that are related to malicious or other human activities. (102)

In identifying who the human *threat agents* are, you need to consider: (103)

a) who might consider it worth their while to attempt to compromise the identified assets, for whatever reasons;

b) who would be in a position to attempt to compromise those assets - in other words, who could gain access to the IT systems which store, process or transmit the asset;

c) what is likely to be their level of technical expertise, opportunities, available resources (e.g. automated tools for hacking and probing networks) and motivation.

Non-human sources of threats, as well as threats *unintentionally* arising from human sources (i.e. by accident), should also be considered where these could lead to compromise of assets. (104)

Identifying the attack methods

Having identified the assets to be protected and the threat agents, the next step is to identify the possible attack methods which could lead to a compromise of the assets. This will be based on what is known regarding the TOE security environment, for example: (105)

a) potential vulnerabilities to the assets which a threat agent could exploit;

b) the capabilities of attackers who have access to the TOE security environment.

Potential vulnerabilities to an organisation's assets may be identified by a vulnerability analysis of the TOE security environment (note however that such an analysis is not within the scope of ISO/IEC 15408), taking into account the identified environmental assumptions. However, you should note that such an analysis may not identify all vulnerabilities, and should not therefore underestimate the possibility of new and undiscovered threats. (106)

The role of risk analysis in threat identification

Risk analysis methods may be helpful in the process of threat identification, but such methods are not defined in ISO/IEC 15408. The risk analysis process is also likely to have a bearing on the identification of the security objectives for the TOE and its environment (see Chapter 4), and the required level of assurance in the countermeasures proposed to address the threats (see Chapter 5). Such methods may consider: (107)

a) the probability and consequences of compromise of the assets, taking into account:

   - the possible attack methods identified,
   - the likelihood of the attack proving to be successful, and
   - the consequences of any damage that may be caused (including the expected magnitude of tangible loss arising from a successful attack);

b) other constraints such as legal requirements and cost.

4.3.2 How should threats be specified?

Having identified the threats to be addressed by the TOE or its environment, the next step is to specify them in the PP or ST. As noted above, the *TOE Security Environment* section should be a clear and concise statement of the security needs, and a clear and concise specification of threats is an essential part of this. (108)

In order to provide a *clear* specification of a threat, you should include the following details (identified as described in section 4.3.1 above): (109)

a) the threat agent (e.g. an authorised user of the TOE);

b) the assets subject to the attack (e.g. sensitive data);

c) the attack method employed (e.g. impersonation of an authorised user of the TOE).

For example: (110)

> *An attacker may gain unauthorised access to information or resources by impersonating an authorised user of the TOE.*
>
> *An authorised user of the TOE may gain unauthorised access to information or resources by impersonating another authorised user.*

It will help the reader to understand the threat if the threat description is accompanied by an explanation of any terms used within the description of the threat, and the scope of the threat in terms of the assets at risk of compromise and specific attack methods that the threat agent might use. For example, in the case of the threats above it may be usefully clarified that the assets at risk are the information and resources which the (impersonated) user has the right to access. (111)

In order to help ensure you have a *concise* statement of threats, as far as possible the threat descriptions should be *disjoint*. In other words, there should be minimal overlap between different threats. This will help avoid potential confusion on the part of the reader of the PP or ST as well as helping to simplify the PP or ST rationale by avoiding needless repetition. (112)

Overlap between threats can be more easily avoided if you specify all threats at the same level of detail. For example, don't specify a threat describing a detailed attack method against a specific asset if this is a specific attack scenario that is already associated with a more general threat stated elsewhere in the PP or ST. (113)

Each threat should be uniquely labelled for ease of reference (for example, in those parts of PP rationale which show how the specified security objectives address the threats). Possible options are: (114)

a) sequential numbering of threats (e.g. T1, T2, T3, and so on);

b) a unique label providing a brief but meaningful 'name' for the threat (e.g. as used in the example threats given in annex B).

The advantage of the second option over the first is that the label is likely to be more meaningful and memorable than a mere number. The disadvantage of this approach is that it may not be possible (due to practical constraints limiting the number of characters in the label) to assign a meaningful label in all cases; indeed in some cases a label may actually be misleading or ambiguous. (115)

The threat descriptions should only refer to potential events which could *directly* compromise the assets requiring protection. It is therefore recommended that you do not include 'threats' of the form *There may be security flaws in the TOE.* Such a 'threat' does not help the reader to understand what the security need is, especially since it applies to any TOE. Moreover, it is not an event that can actually be addressed by the TOE or by any non-technical measures that can be taken within the TOE security environment; rather, it can only be addressed by actions taken by those who develop and evaluate the TOE. (116)

The introduction of countermeasures to the threats may introduce detailed attacks that may lead indirectly to compromise of the assets, for example bypassing or tampering attacks against the TOE security functions. Caution is advised when considering such *indirect* threats to the assets; in particular you should ensure that any such threats: (117)

a) will not, as a result of their inclusion in the *TOE Security Environment* section, confuse the reader by anticipating details of the TOE implementation;

b) do not already fall within the scope of an existing threat.

For example, if threat X could compromise asset Y, then it follows that any attempt to bypass the countermeasure to threat X may also lead to compromise of asset Y. Therefore, bypass of the countermeasure to threat X may be an attack method that is already implicitly within the scope of threat X, and hence (for the sake of brevity in the statement of TOE security environment) does not need to be stated explicitly as a separate threat. (118)

(It should also be noted that you will need to consider attacks against the countermeasures of the TOE, such as bypassing and tampering, when you come to select the IT security requirements, which ISO/IEC 15408 requires to be mutually supportive: see section 8.3.4. Any feasible attacks against the TOE security functions should also be discovered during the evaluation of the TOE.)(119)

Example threats are presented in Annex B of this guide. (120)

4.3.3 Completing the statement of threats

ISO/IEC 15408 requires the *TOE Security Environment* section to include all threats to the assets that are relevant for secure TOE operation ([15408-1], subclause B.2.4, page 39). The threats that are of principal interest are those that will be countered by the TOE (which will often be in association with procedural or other non-technical countermeasures). However, for completeness, the PP or ST may need to include some threats that are not at all addressed by the TOE, for example because of attack methods or threat agents against which the TOE offers no protection. (121)

Examples of threats that are relevant to secure operation of the TOE, but which might not be addressed by the TOE, might include: (122)

a) physical attack against the TOE;

b) abuse of trust by highly privileged users;

c) improper administration and operation of the TOE by careless or improperly trained administrators.

The decision as to which threats are to be addressed by the TOE, and which (if any) are only addressed by the environment, will not (of course) be made until the security objectives are finalised. (123)

It should be noted that the identified environmental assumptions may preclude certain threats that would otherwise have been considered relevant to the secure operation of the TOE. It follows from this that the PP or ST author has a certain amount of freedom in deciding whether such aspects are dealt with in the environmental assumptions or in the statement of threats to be countered by the operating environment. Either approach is acceptable since both assumptions and threats have to be mapped onto the security objectives which uphold or address them. The choice between these two alternatives should therefore be made on the basis of which approach best helps the reader to understand the security needs. As a general rule, specific attacks should be handled as threats, whilst more general forms of attack may be best handled as assumptions. Whichever approach is adopted, however, it is important that the issue is only stated once. (124)

4.4 How to Identify and Specify the Organisational Security Policies

ISO/IEC 15408 requires the *TOE Security Environment* section to contain a description of any OSPs with which the TOE must comply ([15408-1], subclause B.2.4, page 39). However, ISO/IEC 15408 goes on to say that the statement of OSPs may be omitted if the security objectives are derived solely from the threats: in other words, where the 'security needs' are defined in full by the threats. (125)

As indicated in section 4.3 above, a PP and ST author should review any OSPs against the existing and relevant threats to the assets before including them in the PP or ST. (126)

An OSP is defined as one or more rules, procedures and practices imposed by an organisation ([15408-1], subclause 2.3, page 5). An OSP may need to be applied by the TOE or its environment, or by some combination of the two. (127)

If your PP or ST specifies OSPs as well as threats, you should remember the requirement that the *TOE Security Environment* section provide a concise statement of the security needs: little useful purpose is served by including a OSP which is simply a restatement of a threat in a different form (unless of course you have no choice in the matter because the relevant organisation mandates an OSP which is a restatement of an existing threat). (128)

For example, if you have identified a threat which states (129)

> *An unauthorised person may gain logical access to the TOE*

then there is little to be gained from including an OSP which states

> *Legitimate users of the TOE must be identified before TOE access can be granted.*

This OSP does not only (in effect) restate the threat in a different form, it also pre-empts the definition of security objectives which provide the intended response to the security needs. Your PP or ST will be easier to follow if you only state the problem once. (130)

As a general rule, it will be appropriate to specify OSPs where the TOE is intended for use by a specific organisation or a type of organisation, or where there is a need for the TOE to implement a set of rules that cannot be sensibly included within or implied by a threat description. Examples include: (131)

a) identification of information flow control rules to be applied;

b) identification of access control rules to be applied;

c) definition of an organisation's security policy with respect to security audit;

d) solution techniques mandated by the organisation, e.g. use of specified approved cryptographic algorithms, or conformance with identified standards.

As with the threats, each OSP should be uniquely labelled for ease of reference. (132)

Example OSPs are presented in Annex B of this guide. (133)

5 The Security Objectives

5.1 Introduction

This chapter provides guidance on the identification and specification of security objectives in a PP or ST, the requirements for which are described in [15408-1] subclauses B.2.5 and C.2.5. (134)

The *security objectives* provide a *concise statement of the intended response to the security problem* ([15408-3], subclause 4.4, page 31). In other words, having stated (in the *TOE Security Environment* section) what the security needs are, you now need to give an indication of the extent to which they will be addressed by the TOE and its environment, in the form of a statement of security objectives. This is illustrated in Figure 2 below. (135)

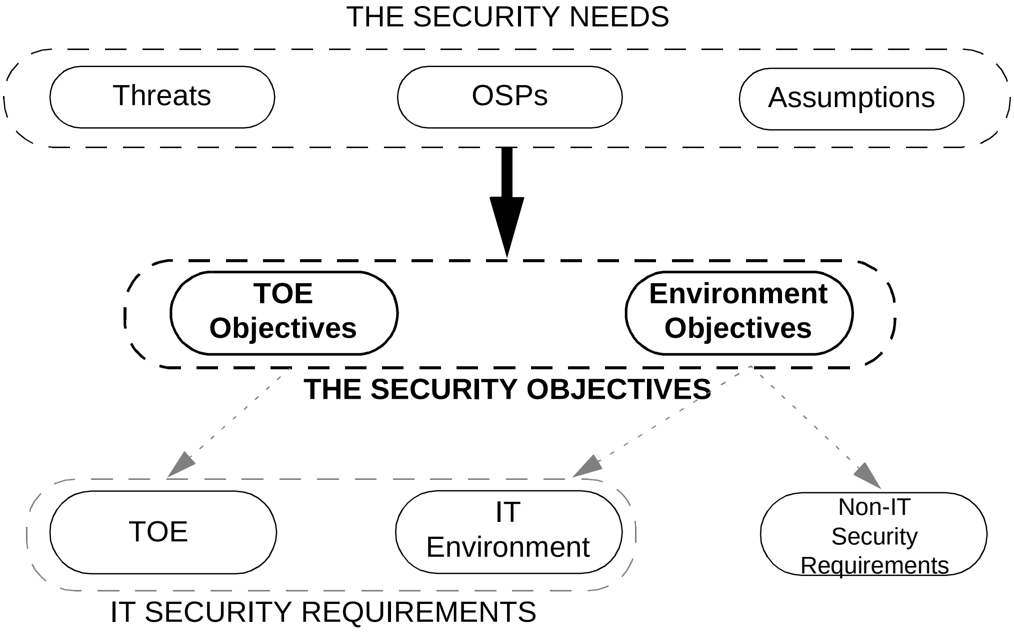

Figure 2 - Role of the Security Objectives

Figure 2 illustrates the two types of security objectives which ISO/IEC 15408 requires to be clearly distinguished in a PP or ST: (136)

a) Security objectives for the TOE, which will be satisfied by technical (IT) countermeasures implemented by the TOE;

b) Security objectives for the environment, which are to be satisfied by either technical measures implemented by the IT environment, or by non-IT (e.g. procedural) measures.

Thus the statement of security objectives serves to outline what the TOE will and will not do within the context of the TOE security environment. By clearly dividing responsibility for meeting the security needs between the TOE and its environment, the risk to the assets requiring protection can be mitigated. Furthermore, in defining this division of responsibility, the statement of security objectives will scope the evaluation of the TOE; this is because the security objectives for the TOE drive both the selection of security functional requirements that are needed to fulfil the TOE's responsibilities in meeting the security needs, and also the determination of the level of assurance needed in the security functions required of the TOE. (137)

5.2 How to Specify Security Objectives for the TOE

The security objectives for the TOE must state (to the extent desired by the PP or ST author) what the responsibility of the TOE is in countering the threats and in supporting the OSPs. As illustrated in Figure 2 above, the security objectives for the TOE may be viewed as providing the reader with a 'stepping stone' (or bridge) from the identified security needs to the IT security requirements, and this should always be borne in mind when specifying the security objectives for the TOE. (138)

Because of the pivotal role played by the security objectives in the PP or ST, the question of what level of detail is appropriate in a statement of security objectives is important. ISO/IEC 15408 gives a strong hint by saying (as pointed out above) that security objectives are intended to be *concise*. In practice, you need to strike a balance between the following two considerations: (139)

a) The security objectives should help the reader to understand the extent to which the security needs are to be addressed by the TOE, without delving into implementation detail; ideally, the security objectives for the TOE should be implementation-independent. The focus is thus on *what* the solution intends to achieve rather than *how* it is achieved.

b) At the same time, you should ensure that the defined security objectives do not just repeat the information contained within the threats and OSPs (albeit in a slightly different form).

The test of whether you have pitched your security objectives at the right level of detail will ultimately come when you construct the rationale for the security objectives and the IT security requirements. If one step in the rationale is trivial whilst the other is comparatively difficult, it is likely that your security objectives are either too detailed or too abstract, depending on which step is the easier. (140)

As will become clear in the next section of this Guide, a well-defined set of security objectives for the TOE will help ensure that the IT security requirements selected to meet them are not excessive - either in terms of the security functional requirements (see section 6.2.1) or the security assurance requirements (see section 6.3.1). This in turn will serve to minimise the cost and timescales of the TOE evaluation. (141)

Broadly speaking, three types of security objective can be identified to address the identified threats: (142)

a) *Preventative* objectives, which prevent a threat from being carried out, or limit the ways in which it can be carried out;

b) *Detective* objectives, which provide the means to detect and monitor the occurrence of events relevant to the secure operation of the TOE;

c) *Corrective* objectives, which require the TOE to take action in response to potential security violations or other undesirable events, in order to preserve or return to a secure state and/or limit any damage caused.

An example of a *preventative* security objective is the following, which identifies the need for identification and authentication of users of the TOE: (143)

> *The TOE will ensure that each user is uniquely identified, and that the claimed identity is authenticated, before the user is granted access to the TOE facilities.*

Access control and information flow control security objectives also fall into the *preventative* category. Where the security needs indicate that the TOE should enforce more than one access control or information flow control policy, it is recommended that you identify distinct security objectives for each policy. Such an approach will help simplify the security requirements rationale. (144)

An example of a *detective* security objective is the following, which identifies the need for the TOE to provide a non-repudiation of origin capability: (145)

> *The TOE will provide the means by which a recipient of information can generate evidence which can be used as proof of the origin of that information.*

An example of a *corrective* security objective is the following, which identifies the need for the TOE to respond to detected intrusions: (146)

> *The TOE will, upon detection of events that are indicative of an imminent security violation, take appropriate steps to curtail the attack with a minimum of disruption to the service provided to other TOE users.*

Where possible, the security objectives should aim to informally quantify the minimal effectiveness expected, thus leaving little doubt as to what level of effectiveness must be justified in the PP or ST rationale. Quantities may be stated: (147)

a) in relative terms, e.g. to environmental conditions or to a previous situation;

b) in absolute numeric terms.

Clearly, specifying absolute numeric values is the most precise option, but is also the most difficult to assess in terms of effectiveness. (148)

If your PP or ST is being written where the SFRs are already known, a useful starting point may be to define one security objective for the TOE corresponding to each of the major groupings of security functional requirements that will be specified in the PP or ST. One benefit of this approach will be to simplify the construction of the security requirements rationale. If this approach is adopted, you still ensure that the defined security objectives comply with the guidance in this section. In particular, you should ensure that the security objectives do not contain unnecessary implementation detail. (149)

Examples of security objectives are provided in Annex B of this guide. (150)

ISO/IEC 15408 requires that security objectives for the TOE are clearly traced to the relevant threats and OSPs ([15408-1], subclause B.2.5, page 39). Therefore, you need to ensure that: (151)

a) each identified threat to be countered in full or in part by the TOE is addressed by at least one security objective for the TOE;

b) each identified OSP to be met in full or in part by the TOE is addressed by at least one security objective for the TOE.

This traceability may be provided (for example) by means of textual cross-references or by mappings in tabular form. Whilst the information required may be provided in the rationale (see, Chapters 8 and 9), it may be more helpful to the reader of the PP or ST if the mappings are provided in the security objectives section. Where a security objective is included to comply with an OSP, it may be appropriate to reference the OSP rather than repeat in full the rules to be implemented (e.g. as with O.DAC in the examples in Annex B). (152)

As with threats and OSPs, the security objectives for the TOE should be uniquely labelled for ease of reference. Again, the labelling convention may be based on sequential numbering (e.g. O1, O2, O3, and so on) or the use of brief but meaningful names (e.g. as in the examples presented in Annex B). (153)

5.3 How to Specify Security Objectives for the Environment

The *security objectives for the environment* include any security objectives that are to be satisfied by the IT environment, as well as by procedural or other non-technical measures to be implemented within the operating environment of the TOE. In other words, security objectives for the environment can either be IT or non-IT. (154)

Security objectives for the environment will have to be identified to address those aspects of the security needs that the TOE will not (or cannot) be expected to do. In particular, security objectives for the environment will be needed to: (155)

a) counter threats (or aspects of threats) that are not countered by the TOE;

b) help satisfy OSPs that are not fully satisfied by the TOE;

c) support the identified security objectives for the TOE by helping to counter the threats or satisfy the OSPs;

d) ensure that identified environmental assumptions are upheld.

An appropriate starting point to the identification process might therefore be to compile a list of security objectives by taking each threat, OSP and assumption that is not to be fully addressed by the TOE in turn, and for each such aspect of the TOE security environment to either: (156)

a) add a new security objective to the list to address that aspect; or

b) map an existing security objective to that aspect if an appropriate one has already been identified (possibly rewording the security objective to extend its scope).

This list should then be refined when you formulate the security objectives rationale, since this may lead to the identification of additional security objectives that are needed to ensure that the security needs are suitably met (in terms of the threats to be countered and the OSPs and assumptions to be covered). (157)

The identification process should be carried out in conjunction with the identification of security objectives for the TOE. The statement of security objectives as a whole should then be reviewed to ensure that the division of responsibilities between the TOE and its environment is appropriate, i.e. such that: (158)

a) the security objectives for the TOE will not lead to a set of IT security requirements that are unduly expensive to evaluate;

b) the security objectives for the environment will not lead to a set of procedural or other non-IT security requirements that will be impractical to implement, or will be unduly restrictive to the TOE users.

Typical examples of (non-IT) security objectives for the environment include: (159)

a) establishment and implementation of procedures to ensure that the TOE will be used in a secure manner (and in particular in accordance with the environmental assumptions);

b) objectives for education and training of administrators and users in sound security practices.

The statement of security objectives for the environment should therefore include any security objectives relating to management activities needed to ensure that the security services to be provided by the TOE are effective. In some cases, the required management activity is obvious, and can be conveniently expressed in the form of a (non-IT) security objective for the environment (e.g. regarding the need for proper management of the audit functions). In other cases the required management activity may depend on the detailed security requirements used to implement the TOE security objectives. For example, the 'identification and authentication' security objective given at paragraph 143 above might be implemented by user passwords. This would imply a requirement for users to ensure their passwords are not disclosed to other individuals, which would properly be expressed as a security requirement for the non-IT environment (see section 6.5.2) which refines the security objective for the environment. (160)

ISO/IEC 15408 states that when a threat or OSP is to be covered partly by the TOE and partly by its environment, the related security objective is to be repeated in each category ([15408-1], subclause B.2.5, page 39). This might be appropriate in the case of the identification and authentication security objective identified above, where the relevant threat can only be countered by the TOE with appropriate support from management activity within the environment, e.g. management of authentication data such as passwords. Thus the security objective might be stated in the following terms: (161)

> *The TOE, with support from its environment, will ensure that each user is uniquely identified, and that the claimed identity is authenticated, before the user is granted access to the TOE facilities.*

In cases where it is possible to clearly divide responsibility between the TOE and its environment, such repetition of security objectives in both categories will clearly not be necessary. An example would be the identification of security objectives for security audit, where the TOE is assigned responsibility for generating and collecting the data, and the environment is assigned responsibility for the supporting management activity, e.g. analysis of the data generated. (162)

A typical example of an IT security objective for the environment is a security objective for an underlying operating system to identify and authenticate TOE users. (Such dependencies on the

IT environment will be refined in the IT security requirements for the environment: see section 6.5.1). (163)

As with the security objectives for the TOE, it is recommended that the security objectives for the environment are uniquely labelled for ease of reference. It may be helpful if you adopt a labelling convention which clearly distinguishes security objectives for the environment from the security objectives for the TOE. If a numbering convention is used, there should be separate numbering for the two types of security objective (for example, security objectives for the environment could be numbered OE1, OE2, OE3, and so on). (164)

Example environmental security objectives are presented in Annex B of this Guide. (165)

6 Security Requirements

6.1 Introduction

This chapter provides guidance on the specification of IT security requirements in a PP or ST. This guidance applies to both TOE security requirements and to security requirements for the IT environment. Security requirements for the non-IT environment (not required to be a formal part of a PP or ST) are also briefly discussed. (166)

The following types of IT security requirements are specified in a PP or ST: (167)

a) Security Functional Requirements (SFRs) on the TOE. These identify the requirements for security functions which the TOE must provide to ensure that the security objectives for the TOE are achieved.

b) Security Assurance Requirements (SARs) on the TOE. These identify the required level of assurance in the implementation of the SFRs.

c) Security Requirements on the IT environment. These define any functional and assurance requirements to be satisfied by the IT environment (i.e. by hardware, firmware and/or software external to the TOE), which are needed in order to ensure that the security objectives for the TOE are achieved.

This is illustrated in Figure 3 below. (168)

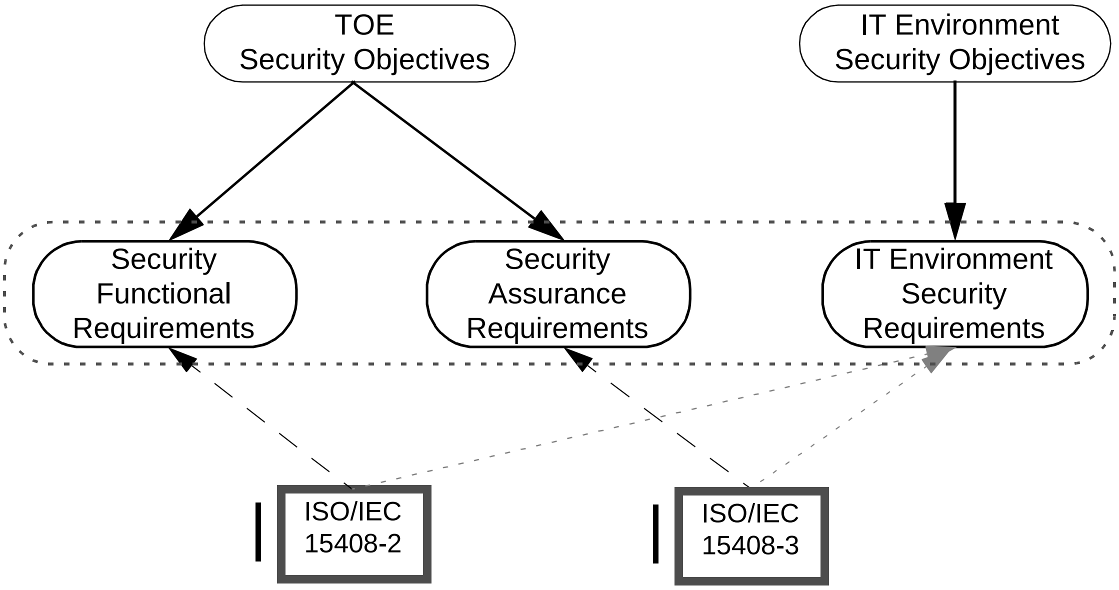
TOE Security Objectives
IT Environment Security Objectives
Security Functional Requirements
Security Assurance Requirements
IT Environment Security Requirements
ISO/IEC 15408-2
ISO/IEC 15408-3

Figure 3 - Derivation of IT Security Requirements

In addition to functional and assurance requirements, the IT security requirements section of a PP or ST is required (where appropriate) to specify a minimum strength of TOE security function level, with explicit strength claims where relevant (see [15408-1] subclauses B.2.6 and C.2.6). (169)

As Figure 3 shows, a significant characteristic of the IT security requirements is that they are intended to be constructed, where possible, using the catalogue of functional components defined in [15408-2] or the catalogue of assurance components defined in [15408-3], as appropriate. The intent of ISO/IEC 15408 here is to ensure a degree of standardisation in the way the IT security requirements are presented. The use of this 'common language' for expressing IT security requirements is thus intended to facilitate comparison between PPs and STs. (170)

However, ISO/IEC 15408 recognises that there may be cases where there is no appropriate functional or assurance component in [15408-2] or [15408-3]. In this case, the IT security requirements may be stated explicitly without reference to ISO/IEC 15408; however, such IT security requirements must be unambiguous, evaluatable, and expressed in a similar style to existing ISO/IEC 15408 components. Section 6.2.5 provides guidance where no appropriate functional components can be identified in [15408-2]; section 6.3.3 provides similar guidance in respect of assurance components. (171)

ISO/IEC 15408 permits a degree of flexibility in the way the SFRs and SARs are specified by allowing a set of *operations* to be performed on them to tailor the security requirement appropriately - namely assignment, iteration, selection and refinement. Section 6.2.2 below provides guidance on the use of operations on ISO/IEC 15408 functional components. Section 6.3.2 does the same for ISO/IEC 15408 assurance components. (172)

A final point to note is that each security requirements component in [15408-2] and [15408-3] is assigned its own unique reference in ISO/IEC 15408, based on a defined taxonomy. For example, the component FAU_GEN.1.2 has the following meaning: (173)

a) 'F' indicates it is a *functional* requirement;

b) 'AU' indicates it belongs to the *security audit* class of SFRs;

c) 'GEN' indicates it belongs to the *security audit data generation* family within that class;

d) '1' indicates it belongs to the *audit data generation* component within that family;

e) '2' indicates it is the second *element* within that component.

SFRs and SARs are selected at the *component* level: all defined elements within that component have to be included in the PP or ST if the component is to be included. There are two types of *relationships* between components which you need to be aware of, as these have a bearing on the process of selecting the IT security requirements: (174)

a) Components within a family may have an *hierarchic* relationship, indicating that one component includes all requirement elements specified in another component in that family. For example, FAU_STG.4 is hierarchic to FAU_STG.3 because all functional elements defined in the latter are also included in the former. However, FAU_STG.4 is not hierarchic to FAU_STG.1, and it is therefore possible to include both components in the same PP or ST.

b) Components may have defined *dependencies* on any component in any other family. For example, FIA_UAU.1 (which requires authentication of any user's claimed identity) has a dependency on FIA_UID.1 (which requires users to be identified). These components must also be included in a PP or ST, unless the dependencies can be shown not to be relevant to the threats and security objectives.

6.2 How To Specify Security Functional Requirements in a PP

6.2.1 How should Security Functional Requirements be selected?

Having defined the security objectives for the TOE in response to the identified security needs, you now need to elaborate on how these security objectives are to be met. This is done by selecting an appropriate set of SFRs which, as stated above, is done at the *component* level. Of course, the SFR selection process will be significantly easier if pre-defined functional packages are available that are relevant to the security objectives for the TOE (see Chapter 11). (175)

There are several stages to the process of selecting the SFRs for a PP. In considering the selection process, it is helpful to distinguish between the following two types of SFR: (176)

a) *principal* SFRs, which *directly* satisfy the identified security objectives for the TOE;

b) *supporting* SFRs, which do not *directly* satisfy the security objectives for the TOE, but which nonetheless provide support to the *principal* SFRs, and hence *indirectly* help satisfy the relevant security objectives for the TOE.

Whilst ISO/IEC 15408 does not *explicitly* distinguish between these two types of SFRs, such a distinction is *implicit* in the consideration of such things as dependencies between functional components, and the demonstration of mutual support between SFRs. Therefore, whilst there is no need for you to explicitly categorise the SFRs as *principal* or *supporting* in the PP, recognising that there are these two types of SFR will be of significant benefit when you come to write the PP Rationale. (177)

The first stage in the SFR selection process is thus, for each security objective for the TOE, to identify the *principal* SFRs which directly satisfy them. Once a complete set of *principal* SFRs has been established, there then follows an iterative process whereby the complete set of *supporting* SFRs are identified. As described above, all SFRs (whether *principal* or *supporting*) should, where possible, be expressed using appropriate functional components from [15408-2]. Annex B provides guidance identifying which functional components should be used to express common security functional requirements. When selecting functional components from [15408-2], you should also consult the guidance contained in the annexes to [15408-2] as to whether the component would be appropriate, and how it should be interpreted. (178)

The relationship between these two types of SFR is illustrated in Figure 4 below. It may be noted that this relationship is relevant to the PP rationale, which, *inter alia*, is required to demonstrate mutual support between the SFRs (see section 8.3.4). This will involve providing an explanation of the nature of the support provided by *supporting* SFRs in helping to ensure that the security objectives for the TOE are met. (179)

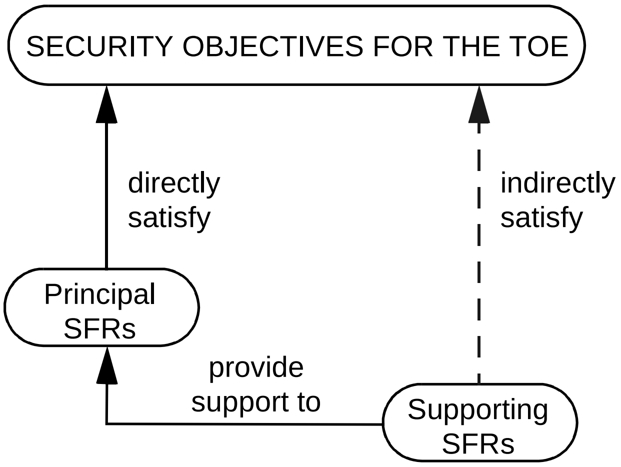

Figure 4 - Role of Principal and Supporting SFRs

There are three stages involved in identifying the complete set of *supporting* SFRs: (180)

a) Identify the additional SFRs needed to satisfy (where you consider it appropriate) the dependencies (as defined in [15408-2] for the relevant functional components) of all *principal* SFRs. This includes any dependencies of the *supporting* SFRs identified during this stage.

b) Identify any additional SFRs that are necessary to ensure that the security objectives for the TOE are achieved. This will include SFRs needed to defend the *principal SFRs* against composite attacks that first defeat the function, then mount the threat the function is intended to counter.

c) Identify the additional SFRs needed to satisfy (where you consider it appropriate) the dependencies of those *supporting* SFRs selected during the second and third stages.

The identification of *supporting* SFRs to satisfy the dependencies as identified in [15408-2] is likely to be an iterative process, for example: (181)

a) Suppose that the PP includes a security objective requiring the TOE to provide specific responses to the detection of events indicative of an imminent security violation. This leads to the inclusion of a *principal* SFR based on the FAU_ARP.1 (Security Alarms) component.

b) According to [15408-2], FAU_ARP.1 has a dependency on FAU_SAA.1 (Potential Violation Analysis) which should also be included as a *supporting* SFR.

c) FAU_SAA.1 has a dependency on FAU_GEN.1 (Audit Data Generation).

d) FAU_GEN.1 has a dependency on FPT_STM.1 (Reliable Time Stamps).

e) FPT_STM.1 introduces no requirements for additional functional components.

It should be noted that ISO/IEC 15408 permits you to leave some dependencies ‘unsatisfied’, provided you explain why the relevant SFRs are not required to satisfy the security objectives (and hence address the security needs). (182)

Dependencies should be applied in a consistent manner. For example, in the case of FAU_ARP.1, consistency is ensured by the nature of the requirements (FAU_ARP.1 depends on the expectation of a potential security violation that is defined by application of FAU_SAA.1.2). (183)

For other components, consistency may be more problematic. For example, in the case of FDP_ACC.1, the PP will identify the particular access control SFP to which it relates. In satisfying the dependency of FDP_ACC.1 on FDP_ACF.1, it must be ensured that FDP_ACF.1 is applied to the same access control SFP that was used for FDP_ACC.1. If the iteration operation is applied to FDP_ACC.1 for different access control SFPs, the dependency on FDP_ACF.1 will need to be satisfied in respect of each such access control SFP. (184)

The identification of additional *supporting* SFRs (i.e. those that are not identified as dependencies in [15408-2]) involves identifying any other SFRs which you consider to be necessary to support the achievement of the security objectives for the TOE. Such SFRs will typically provide support by reducing the options or opportunities available to an attacker, or by increasing the level of expertise or resources an attacker must have to mount a successful attack. The following should be considered in the light of the security needs and the security objectives: (185)

a) SFRs based on relevant components from the same class in [15408-2]. For example if the component FAU_GEN.1 (Audit Data Generation) is included then this may imply a need to create and maintain a secure audit trail to store the data generated (requiring one or more functional components from the FAU_STG family) and a need for tools to review the generated audit data (requiring one or more functional components from the FAU_SAR family). Alternatively, the generated data may be exported to another system for review.

b) SFRs based on relevant components from the FPT (Protection of the TOE Security Functions) class. Such SFRs will typically protect the integrity and/or availability of the TSF or TSF data on which the other SFRs rely. Examples include FPT_AMT.1 (Abstract Machine Testing) and components from the FPT_SEP (Domain Separation) family, which may be required to support the security objectives where there is an identified need to protect the TSF against such things as TSF failure, corruption, or modification (possibly by malicious means).

c) SFRs based on relevant components from the FMT (Security Management) class. These components will be used to specify any necessary supporting security management SFRs. An example of this would be FMT_REV.1 which addresses the revocation of security attributes, and may be considered relevant where SFRs are included that deal with security attributes (e.g. access control).

The selection of these *supporting* SFRs should always be done in the light of the security objectives, in particular taking into account the need to end up with a set of SFRs which form a mutually supportive and integrated and effective whole. The process of constructing the PP rationale may therefore have a significant influence on this selection process. You are strongly advised to avoid including *supporting* SFRs that are not needed to achieve the security objectives, because this will only serve to limit the acceptability of the PP given that: (186)

a) some TOEs may not be able to meet such SFRs;

b) increasing the number of SFRs will increase the cost of evaluation against the PP.

If the PP is being constructed using a related PP as a basis, the process for selection of SFRs should be simplified considerably. However, the new PP should include different SFRs where appropriate so as to take into account any differences between the TOE security environment and/ or security objectives in the two PPs. (187)

6.2.2 How To Perform Operations on Security Functional Requirements

As stated in section 6.1 above (see also [15408-2] subclause 2.1.4), some functional components include permitted operations which may require the PP author to tailor the security requirement as appropriate for the PP. These operations are: (188)

a) *assignment*, allowing the specification of an identified parameter (which may in some cases be a null value);

b) *iteration*, allowing multiple use of the same functional component to express different requirements;

c) *selection*, allowing the specification of one or more elements from a given list;

d) *refinement*, allowing the addition of details to the security requirement, thereby restricting the possible set of acceptable solutions without introducing any new dependencies on other SFRs.

The *iteration* operation is often needed to express SFRs using components in the FMT (Security Management) class, which are called up as dependencies by many different functional components in [15408-2]. In order to satisfy such dependencies, it will typically be necessary to use the same component, with the assignment and selection operations completed differently. For example, FMT_MSA.1 may be iterated a number of times to define distinct SFRs relating to the management of different types of security attributes. Similarly, it may be desirable to make multiple use of components from the FDP_ACC and FDP_ACF families in the case where a TOE is required to enforce different access control policies, e.g. DAC and RBAC. (189)

You are encouraged to use the iteration operation where the clarity of the PP can be enhanced, e.g. to break down a complex and unwieldy SFR into distinct and manageable functional requirements. Use of the iteration operation does, however, pose other potential problems when presenting the SFRs in the PP or ST, as will be seen in section 6.2.6 below. (190)

For each SFR you have included in the PP, you need to make a judgement as to whether to: (191)

a) complete any *assignments* or *selections* included in the functional component used to express the SFR;

b) specify any *refinement* of the SFR.

Assignment and selection

An assignment or selection operation is completed if it leaves no specification decisions to the ST author as to how the functional component is to be tailored to meet the security objectives (other than the possibility of refinement). In other words, there are no aspects (insofar as the operation is concerned) that are ‘to be defined’ by the ST author. (192)

The choice as to whether you should complete individual *assignments* or *selections* will require you to balance the following needs: (193)

a) A PP should be *implementation-independent*: over-specification through completion of operations may unduly restrict the number of TOEs that might be able to claim conformance with the PP.

b) The following statement made in [15408-1], subclause B.2.6, page 41:

> *When requirements components that specify required operations (assignment or selection) are selected, the PP shall use those operations to amplify the requirements to the level of detail necessary to demonstrate that the security objectives are met.*

Therefore, it is necessary to complete assignment and selection operations to the extent needed to meet the security objectives. A critical test will come when you construct the security requirements rationale: the arguments you present to demonstrate the suitability of the IT security requirements to meet the security objectives should not rely on details that have not been specified in the SFRs. For example, in the case of an access control SFR based on FDP_ACF.1, you may consider it appropriate to leave the specification of access control rules entirely in the hands of the ST author if such rules are already defined in an OSP which the relevant (access control) security objective is intended to meet. (194)

One technique that you are strongly recommended to use in order to solve the above problem is that of *partially* completing the operations. By adopting this approach you can give maximum flexibility to the ST author, whilst at the same time precluding potential choices for assignments or selections that would not be consistent with the security objectives for the TOE. (195)

For example, in the following SFR (based on FAU_STG.4.1), the selection operation has been partially completed by precluding selection of the option ‘ignore auditable events’, which the PP author has judged to be inconsistent with the security objectives for the TOE. The SFR therefore presents the ST author with a choice of two (rather than three) acceptable options: (196)

> The TSF shall [selection: ‘*prevent auditable events, except those taken by the authorised user with special rights’*, ‘*overwrite the oldest stored audit records*’] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

A further example is the following SFR (based on FPT_ITT.1), which illustrates how to partially complete a selection such that one of the permitted options is mandated. FPT_ITT.1 permits the specification of a requirement for protection of transmitted TSF data against disclosure, or modification, or both. In this example the PP author has determined that, in order to satisfy a security objective for the TOE, protection of transmitted TSF data from disclosure is required. However, the PP author does not wish to prevent an ST for a conformant TOE from specifying protection against modification as well. The selection has therefore been partially completed such that selection of the undesirable option (protection against modification alone) is precluded: (197)

> The TSF shall protect TSF data from [selection: ‘*disclosure*’, ‘*disclosure and modification*’] when it is transmitted between separate parts of the TOE.

As a general principle, a *partially* completed selection is valid if the set of options it presents is a subset of the options that are permitted by the original functional component. Similarly, a *partially* completed assignment is valid if the permitted values to complete the assignment are also valid assignments with respect to the original functional component. If for any reason these conditions are not met, then you have ended up with an extended functional component with a different assignment or selection operation. (198)

Completing the operations of assignment and selection is reasonably straightforward. In the case of assignment, you simply need to ensure that the parameter is specified unambiguously. In the case of selection, you simply need to select the appropriate item(s), based on consideration of the security objectives for the TOE. You should, however, consult the guidance given in the annexes to [15408-2] if in doubt. (199)

Where assignment or selection has been performed in a PP, it is recommended that you highlight the text that has been specified (this will be helpful to the reader, and especially to the PP evaluator checking conformance to ISO/IEC 15408). For example FMT_SAE.1.1 could be presented as: (200)

> The TSF shall restrict the capability to specify an expiration time for *user passwords* to *the authorised administrator*.

If an operation is left uncompleted, it is helpful to make it clear that the onus is on the ST author to specify the details. For example, FDP_RIP.1.1 could be specified in a PP as: (201)

> The TSF shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to the following objects [assignment: *list of objects specified by the ST author*].

Any uncompleted (or partially completed) operations should, where appropriate, be accompanied by an explanation, targeted at the ST author, of how the operation should be completed (for example, in the form of an application note). (202)

Refinement

The operation of refinement may be performed on any functional component element, and involves specifying additional technical details which do not levy any new requirements to those specified in the text, but rather restrict the set of acceptable implementations. A refinement is acceptable if meeting the refined requirement also means meeting the unrefined requirement. As a general rule, this operation should be applied sparingly in a PP since this could limit the widespread usage of the PP. Use of refinement may nonetheless be appropriate in the following circumstances: (203)

a) where the PP is being written by an organisation which has specific security requirements that are not included in the appropriate ISO/IEC 15408 Part 2 component, and which cannot be specified through permitted assignment or selection operations;

b) where the selected functional component would permit implementations which would not make sense, or would otherwise be inappropriate, for the type of TOE considered, unless it is refined so as to exclude that possibility;

c) where the readability of the SFR may be improved: see section 6.2.6.

As with assignment and selection operations, it is recommended that you highlight the text that has been specified to assist the reader (and the PP evaluator in particular). (204)

An example of the use of the refinement operation is as follows (based on FMT_MTD.3.1). (205)

> The TSF shall ensure that only secure values are accepted for TSF data.
>
> *Refinement: the TSF shall ensure that the minimum password length enforced by the TOE is configured to a value of at least 6 characters.*

The use of the refinement operation to help clarify SFRs is discussed in section 6.2.6 below. (206)

6.2.3 How should the audit requirements be specified?

If the PP includes auditing requirements (i.e. based on FAU_GEN.1) then ISO/IEC 15408 requires that the minimum set of events which must be auditable, and the minimum information which must be recorded, is specified through the consideration of all other functional requirements included in the PP. (207)

This selection will depend on a number of factors, including: (208)

a) any security policy requirements on security audit, as defined in an OSP;

b) the importance of auditing in achieving the security objectives;

c) the relevance of potential events, and their characteristics, to the security objectives;

d) cost/benefit analysis.

For example, if the TOE is intended to defend against the actions of malicious users or hackers, it is likely that events such as login or access control violations will need to be auditable where the PP includes such SFRs. However, events relating to the use of administrative functions may not need to be auditable, depending on the extent to which an administrator is (or has to be) trusted. (209)

The question of cost/benefit analysis may rest on such issues as: (210)

a) is the benefit of collecting the information worth the impact on performance?

b) if the information is collected, will the administrator have sufficient resources (e.g. tool support) to effectively analyse the data?

c) what are the likely costs of managing or archiving the data collected?

ISO/IEC 15408 identifies three pre-defined levels of auditing, namely *minimum*, *basic*, or *detailed* ([15408-2], subclause 2.1.2.5, page 11): for each such level, [15408-2] tells you which events should be auditable (as a minimum), together with the minimum information to be recorded, based on the functional components included in the PP (see also [15408-2] subclause C.2). These three levels can be broadly characterised as follows: (211)

a) The *minimum* level typically requires only some defined subset of operations or events associated with a given functional component to be auditable. This subset is generally defined to be the most interesting or significant type of event.

b) The *basic* level typically requires all operations or events associated with a given functional component to be auditable, e.g. successful and unsuccessful login attempts.

c) The *detailed* level generally differs from the *basic* level by requiring additional information of interest to be recorded. This level is only likely to be appropriate where the amount of audit data generated is anticipated to be small, or if the data will be subject to analysis by sophisticated audit analysis tools or intrusion detection facilities.

If none of these levels is appropriate, you should select the *not specified* level, and list all required auditable events explicitly in FAU_GEN.1.1c. For example, you might use the *minimum* level for guidance, but choose to deviate from the *minimum* requirements in specific cases because a different subset of operations or events is more relevant to the security objectives, e.g. if FDP_ACF.1 is included in the PP, you may consider that unsuccessful access attempts should be auditable rather than *successful* attempts (which is what [15408-2] requires for the *minimum* level). (212)

You will need to compile a list of auditable events by going through each functional component used in turn; in the case of the pre-defined levels of *minimum, basic* or *detailed*, these are explicitly identified in the *Audit* section included for each family of components. It is recommended that you construct a table, identifying the events and (where appropriate) the additional information to be recorded, which can be referenced by FAU_GEN.1.1 and FAU_GEN.1.2 as appropriate. (213)

6.2.4 How should management requirements be specified?

[15408-2] identifies, in the *Management* section included for each family of components, a list of management activities which should be considered for the component. This may suggest the need to include particular components from the FMT (Security Management) class. However, it is important to note that this section is intended to be *informative*. There is therefore no need to justify any decision not to include particular management components in the PP (unless, of course, they are explicitly identified in the *Dependencies* section within [15408-2]). (214)

Generally speaking, possible management activities are identified where a functional component refers to, or implies the existence of, configurable TSF data which may need to be managed and controlled. For example, the security objectives for the TOE might be undermined if the ability to modify such data was not restricted to administrators of the TOE. Therefore FMT components are often included in order to define *supporting* SFRs, in order to ensure that the security objectives for the TOE are met, and that the SFRs as a whole are mutually supportive (see sections 8.3.1 and 8.3.4). (215)

You should consult the guidance on the FMT class given in [15408-2] Annex H when choosing functional components from this class. (216)

6.2.5 How should SFRs not included in ISO/IEC 15408 Part 2 be specified in a PP?

ISO/IEC 15408 requires that if the PP author wishes to include a functional requirement for which there is no appropriate functional component defined in [15408-2], the resultant SFR should be specified using ISO/IEC 15408 Part 2 components as a model for presentation. (217)

The decision as to whether there is an appropriate functional component in [15408-2] to use can be a difficult one to make, since this requires a high degree of familiarity with its content. It is recommended that you consult the guidance in Annex B which identifies the appropriate functional components to express common security functional requirements. It is often the case that the desired SFR can be obtained through appropriate application of the refinement operation, or of permitted assignment or selection operations. However, it is recommended that you do not attempt to 'shoehorn' an SFR into a functional component if this does not readily lead to the SFR you want, i.e. it results in an SFR whose meaning or intent cannot be readily discerned by the reader, or which (through the use of an inappropriate component) introduces inappropriate dependencies that need to be argued away. (218)

Specifying a new SFR using ISO/IEC 15408 Part 2 functional components as a model for presentation will involve: (219)

a) defining the SFR at a similar level of abstraction as ISO/IEC 15408 Part 2 components;

b) using a similar style and phraseology to ISO/IEC 15408 Part 2 components.

Knowing that a new SFR is of a similar nature to others in an existing class or family helps bound its degree of newness and also may help with specific wording for common concepts that occur throughout that class or family. (220)

Particular characteristics of the style of presentation of functional components in [15408-2] include: (221)

a) most functional requirements begin with the phrase *The TSF shall* or *The TSF shall be able to,* followed by a verb such as *allow, detect, enforce, ensure, limit, monitor, permit, prevent, protect, provide* or *restrict*;

b) the use of standard terms such as *security attribute* or *authorised user*;

c) each element tends to stand on its own and can be understood without reference to previous elements;

d) each security requirement must be evaluatable, i.e. it must be possible to determine whether the requirement has been met by a TOE.

In constructing an explicitly stated SFRs, you should also consider whether the SFR: (222)

a) should incorporate any assignment or selection operations to be completed by the ST author;

b) implies any dependencies on other SFRs which must be satisfied by the PP;

c) describes any events which should be auditable, and if so what information should be recorded for the event;

d) has any implications for security management, e.g. relies on security attributes that need to be managed.

If you believe you have a well-constructed SFR that is not included in [15408-2], and is significantly different from, and would significantly enhance, the existing set of functional components in ISO/IEC 15408, you are advised to submit the SFR for inclusion in the next iteration of that document. (223)

The naming convention for SFRs not based on [15408-2] components should make it clear that such SFRs are extended security requirements. You should take care that such names do not conflict with future ISO/IEC 15408 class, family and component names, e.g. by avoiding short names of the form XXX_YYY. However, if the extended component has been derived from an existing component in [15408-2], it is acceptable for similar (but distinct) naming to be used. (224)

6.2.6 How should the SFRs be presented?

Writing a set of SFRs that are demonstrably compliant with the requirements of ISO/IEC 15408 is not (of course) the *only* aim of the PP author. You should also consider how best to present and express the SFRs such that the general reader can understand what the security requirements mean. There are a number of steps you can take to enhance readability, without compromising compliance with ISO/IEC 15408. (225)

Firstly, group the SFRs under headings which are appropriate for your PP: do not feel constrained to adopt the class, family or component headings used in [15408-2]. (226)

Secondly, do not feel constrained to adopt the functional element labelling system used in [15408-2] for labelling the SFRs in your PP. It is perfectly acceptable to adopt your own labelling system (which may feature more meaningful labels), provided the mapping of SFRs onto the relevant functional component from [15408-2] is demonstrated (e.g. in an annex). Indeed, such an approach is likely to be highly desirable where the PP includes functional components which are invoked several times. This is because the alternative is to have SFRs that do not have unique labels: the lack of unique labels for SFRs presents significant problems when constructing the security requirements rationale. (227)

Thirdly, judicious use of the refinement operation may improve the readability of the SFR by substituting generic terms (such as *security attributes*) with more specific terminology relevant to the type of TOE or security functionality being described. For example, the following SFR is based on FMT_MSA.3.1: (228)

> The TSF shall enforce the *DAC policy* to provide *restrictive* default values for *object permissions*.

In this example, refinement has been used to replace the generic ‘security attributes that are used to enforce the SFP’ with the policy-specific ‘object permissions’. (229)

Any such use of the refinement operation should be clearly highlighted and explained in the PP Rationale (to support evaluation of the PP). (230)

The worked example presented in Annex F illustrates the application of this approach. (231)

6.3 How To Specify Assurance Requirements in a PP

6.3.1 How should Security Assurance Requirements be selected?

The selection of the assurance requirements will require the balancing of several factors including: (232)

a) the value of the assets to be protected and the perceived risk of compromise of those assets;

b) technical feasibility;

c) likely development and evaluation costs;

d) required timescales for development and evaluation of the TOE;

e) perceived market requirement (in the case of products);

f) any identified dependencies of functional components on assurance components.

The greater the value of the assets to be protected, and the greater the risk to those assets, the higher the level of assurance that will be required in the security functions used to protect those assets. This should be reflected in the statement of security objectives. Organisations may define their own policies and rules to determine the level of assurance that is needed to ensure that the risks to their assets are reduced to an acceptable minimised. This may in turn define the required level of assurance in products to be used within that organisation. (233)

Other factors such as costs and timescales will tend to act as a constraint on the level of assurance that is actually achievable in practice. Technical feasibility will be a factor where it is considered impractical to generate the evidence required by specific assurance components. This may be highly relevant for legacy systems (where design documentation is unavailable), or where a high assurance level is ideally required, but it is not technically feasible to generate the required semi-formal or formal evidence within acceptable timescales. Wherever there are practical constraints on the assurance that may be achieved, it may be necessary to accept that the maximum assurance attainable is less than the ideal. Such acceptance of risk should, again, be reflected in the statement of security objectives. (234)

The statement of security objectives may also indicate a need for specific assurance requirements which should be included in the SARs. For example: (235)

a) The security objectives for the TOE may state that the TOE should be resistant to attackers who have a high attack potential. This would be a clear pointer to the inclusion of AVA_VLA.4 which requires such resistance to be demonstrated.

b) The security objectives may indicate that covert channels are a concern, in which case it may be necessary to include a component from the AVA_CCA family to require a covert channel analysis to be performed.

c) The security objectives may note that the security of the TOE is critically dependent on the security of the development environment. This would strongly suggest that the SARs should include a component from the ALC_DVS family to ensure that the security of the development environment is examined.

The selection of the SARs will (of course) be relatively straightforward where it involves simply choosing an appropriate assurance package (see Chapter 11), such as an ISO/IEC 15408 EAL. The definitions and descriptions of the assurance package should be consulted to ensure that the package is appropriate given the statement of security objectives (e.g. in the case of the EALs, see [15408-3] clause 6). It is possible that an assurance package exists that provides broadly the level of assurance that is needed, but is lacking in specific areas when measured against the security objectives. In such cases it would be appropriate to include augmented assurance requirements (i.e. requirements that are additional to those mandated by the package) in order to ensure that the security objectives are satisfied. (236)

Where augmented assurance requirements are specified, the PP author should ensure that the assurance component dependencies are satisfied for the additional requirements. For example, if a PP augments EAL3 with AVA_VLA.2, then it should also augment with ADV_LLD.1 and ADV_IMP.1, as these are not included in EAL3. (237)

6.3.2 How To Perform Operations on Security Assurance Requirements

As indicated in [15408-3] subclause 2.1.4, the assignment and selection operations are not relevant to the assurance components defined in [15408-3]. However, the following operations are possible: (238)

a) *iteration*, allowing multiple use of the same assurance component;

b) *refinement*, allowing the addition of details to the assurance requirement without introducing any new dependencies on other SARs.

In practice, the iteration operation would only be used where it is necessary to apply different refinements to the same assurance component which apply to different parts of a TOE, or where a PP or ST specifies different sets of assurance requirements for different components of a composite TOE (see section 10.2.4). In the latter case, iteration would be necessary for assurance components (whether refined or not) that apply to more than one component of the composite TOE. (239)

Use of the refinement operation on SARs might be used to: (240)

a) constrain the developer actions by mandating such things as the use of specific development tools, methodologies, life-cycle models, analysis techniques, notations, adherence to specific standards, and so on;

b) constrain the performance of the evaluator actions, e.g.

- in the case of ADV_IMP.1, specifying which parts of the TOE implementation representation should be included in the subset examined
- in the case of AVA_VLA.1, identifying specific known vulnerabilities that are considered to be ‘obvious’ in the context of the TOE.

6.3.3 How should SARs not included in ISO/IEC 15408 Part 3 be specified in a PP?

ISO/IEC 15408 requires that if the PP author wishes to include an SAR for which there is no appropriate assurance component defined in [15408-3], the resultant SAR should be specified using ISO/IEC 15408 Part 3 components as a model for presentation. Explicitly stated SARs should provide a definition of the following elements (see [15408-3] subclause 2.1.3.5 for more details): (241)

a) developer actions;

b) requirements for the content and presentation of evidence that a developer must provide;

c) evaluator actions.

Inspection of [15408-3] shows that the first evaluator action associated with an assurance component is generally of the form: (242)

> *The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.*

Therefore, all requirements for content and presentation of evidence should not only be clearly and unambiguously expressed, but also should avoid (as far as possible) requiring subjective judgement on the part of the evaluator. Rather, the SAR should define clear objective criteria against which an evaluator may reach a verdict. You should consider the use of the refinement operation or application notes to provide any clarification of the SAR that is needed in support of this requirement for objective judgement. (243)

To ensure that the explicitly stated SARs are specified in the same style as [15408-3] components, you should ensure that each separable requirement is stated as an individual requirements element ([15408-3], subclause 2.1.4, page 10). You should also, when choosing the wording of the SAR, consult [15408-3] subclause 2.4 which gives a definition of general English terms that are used in a precise way within [15408-3]. (244)

If you believe you have a well-constructed SAR that is not included in [15408-3], and is significantly different from, and would significantly enhance, the existing set of assurance components in ISO/IEC 15408, you are advised to submit the SAR for inclusion in the next iteration of that document. (245)

6.4 How To Specify Security Requirements in an ST

6.4.1 How should SFRs taken from a PP be specified?

Where an ST claims compliance with one or more PPs, it is likely that the SFRs will be specified either completely or mostly by the PP. In such cases, the ST author must decide whether to specify the PP functional requirements in full (in order to ensure all the text is in one place), or whether to simply reference the PP and specify SFRs where these differ from the PP. (246)

In general, the latter approach is recommended since this will simplify the ST. The reader of an ST is more likely to be interested in the IT security functions than in the SFRs. This includes the evaluator of the TOE (since the content of evaluation evidence - such as design, test documentation and guidance documents - is likely to be more easily related to the IT security functions in the TOE summary specification than to the SFRs). The main purpose of specifying SFRs in an ST is to be able to demonstrate traceability back to relevant PPs, and to the SFRs as defined in Part 2 of ISO/IEC 15408. There is indeed a case for relegating the statement of SFRs to an annex so as not to confuse the reader by having two specifications of security functionality in the ST. (247)

It should, however, be noted that some SFRs in the PP may have operations (such as assignment or selection) that are left to the ST author. In such cases it is recommended that the SFR is specified in full, with the completed operations emphasised by suitable typesetting (e.g. using italics). Any necessary explanations should be added using the same typesetting. Such an approach will make it easier for the reader of the ST (and the ST evaluator in particular) to see which operations have been performed, and in which manner. It will also facilitate the construction of the ST rationale (see section 9.3.6). (248)

6.4.2 How should SFRs not in a PP be specified?

In some cases it will be necessary to specify SFRs in an ST where these are not in a corresponding PP. This may be necessary where: (249)

a) there is no appropriate PP available for the TOE to claim compliance with;

b) the sponsor considers that the benefit to be gained by requiring or claiming functionality that is in addition to what is required by the PP is sufficient to justify the additional evaluation cost that would be incurred.

In such cases, the approach to the specification of SFRs is the same as described in the preceding chapter. Where SFRs are specified in addition to those required by a PP, the ST author must ensure that these do not conflict with SFRs in the PP (the ST rationale will need to demonstrate that such conflict does not occur: see chapter 9). (250)

6.4.3 How should SFRs not included in ISO/IEC 15408-2 be specified in an ST?

ISO/IEC 15408 permits the ST author to explicitly state SFRs in an ST without reference to ISO/IEC 15408 Part 2. The guidance given in section 6.2.5 above applies. However, it should be noted that it will not be necessary to specify ISO/IEC 15408 operations such as assignment or selection for SFRs constructed in this way if the SFR is only intended for use in the ST, i.e. there is no intent to reuse the component in other PPs, STs, or functional packages. (251)

6.4.4 How should assurance requirements be specified in an ST?

The principles for the specification of SARs are the same as described previously for PPs. (252)

In practice, it is likely that the SARs in an ST will in many cases be determined by a PP with which conformance is to be claimed, or will be specified in terms of a commonly accepted assurance package (e.g. an ISO/IEC 15408 EAL). It is, nonetheless, possible that an ST author will wish to specify assurance requirements which augment an assurance package or a PP’s SARs. This might occur where the sponsor of the evaluation considers that the benefit to be gained justifies the additional evaluation cost. In such cases, the specification of the SARs should be performed as described in the previous section, and should be demonstrably consistent with the security objectives. (253)

SARs that are not based on assurance components included in [15408-3] may be included in an ST as described in the PP guidance given in section 6.3.3 above. (254)

6.5 Security Requirements on the Environment

6.5.1 Security Requirements on the IT Environment

ISO/IEC 15408 requires that any security requirements on the IT environment are included in the PP or ST. For example: (255)

a) A secure database management system (DBMS) may depend on an underlying operating system to provide identification and authentication of its users, and to prevent users of the operating system from bypassing the DBMS access controls by directly accessing the database files.

b) A smartcard application may rely on an underlying smartcard operating system to provide segregation between different applications (such that another application cannot interfere with its code or data), and may also rely on the tamper-resistant properties of the integrated circuit card itself.

Security requirements on the IT environment may also be specified where there are identified dependencies of [15408-2] components in the PP or ST that are satisfied by the IT environment rather than the TOE. (256)

Note that security requirements on the IT environment are distinguished from environmental assumptions in that: (257)

a) assumptions are axiomatic for the TOE evaluation, and are specified to clearly define the scope of the security needs;

b) security requirements are needed to ensure that the TOE meets its security objectives and hence addresses the security needs, and thus will need to be verified at some point.

In contrast with the TOE security requirements, however, the security requirements on the IT environment are not evaluated (in the TOE evaluation) in the sense of it being confirmed to the required degree of assurance that the IT environment provides the SFRs required of it. Evaluation of the TOE will generally presume that the IT environment provides those SFRs, but some security requirements on the IT environment may be tested as a natural consequence of evaluating the TOE. The required level of assurance must therefore ultimately be established through a separate evaluation of the components of the IT environment that provide the required security functionality. (258)

As with the TOE security requirements, ISO/IEC 15408 indicates that the security requirements on the IT environment should be specified, where feasible, using ISO/IEC 15408 functional and assurance components. The PP or ST must provide justification for any deviation from those components. (259)

In some cases, it may not be appropriate to use ISO/IEC 15408 Part 2 components to express the functional requirements on the IT environment. For example, the functional requirements could be expressed in a PP at a more abstract level than the components defined in [15408-2]. This approach would then allow the ST author flexibility in selecting *how* these high-level (implementation-independent) functional requirements are to be satisfied. (260)

For the ST author, the dependencies will (or should be) known since they relate to a specific TOE in a specific (or presumed) environment. By contrast, a PP author needs to take into account the possibility that conformant TOEs may differ in the extent to which they depend on the IT environment. There are two basic cases: (261)

a) The division of responsibility between the TOE and environment is fully determined. In this case, the security requirements on the IT environments should be specified in one or more sections, using multiple sections if there are multiple components in the IT environment.

b) The division of responsibility between the TOE and environment is not fully constrained by the PP. In this case, there is no distinction between the TOE SFRs and the IT environment SFRs. However, if this approach is adopted, the PP author should ensure that claims of conformance are not open to abuse, e.g. by an ST author whose TOE implements a bare minimum of SFRs, and relies on the IT environment to do the rest.

In the latter case, abuse of PP claims can (of course) be avoided by declaring all SFRs as TOE SFRs. In this event, if a product can only satisfy all the PP’s SFRs in conjunction with its IT environment, conformance can only be claimed for the composite TOE that comprises the product with its IT environment. (262)

In the former case, the PP author should specify a minimum set of functionality which must be provided by the TOE. The judgement regarding the division of responsibility between the TOE and its environment should clearly be based on what is technically feasible, and also the functionality provided by existing products which are intended to comply with the PP. The PP should nonetheless be flexible in allowing a conformant TOE to implement any of the security requirements on the IT environment that are identified in the PP. (263)

The assurance in the implementation of any SFRs provided by the IT environment must be at least equal to those placed on the SFRs provided by the TOE. For example, if a DBMS’s access control functionality is to be assured to EAL4, this would be undermined if the identification and authentication functionality provided by the underlying operating system (on which the DBMS’s access control functionality depends) was only assured to EAL2. (264)

6.5.2 Security requirements for the non-IT environment (Optional)

[15408-1] subclauses B.2.6 and C.2.6 state that security requirements for the non-IT environment are not required to be a formal part of a PP or ST as they do not relate directly to the implementation of the TOE, although ISO/IEC 15408 acknowledges that they may be ‘useful in practice’. (265)

Security requirements for the non-IT environment may be needed in a PP or ST when there are non-IT security objectives whose implementation is not straightforward or when the rationale depends explicitly on how the non-IT security objectives have been realised. The latter case arises when there is a need for detailed co-ordination between the PP/ST’s IT security requirements and associated management techniques, with the two kinds of requirements being at a similar level of abstraction. (266)

Note also that if security requirements for the non-IT environment are needed that are not obvious from the non-IT security objectives, and if these non-obvious requirements are not contained within the PP, then it may be infeasible to demonstrate the suitability of the IT security requirements (see section 8.3.1). (267)

Rather than mix abstraction levels by treating security requirements for the non-IT environment as security objectives or assumptions, it is better to provide a separate section for security requirements for the non-IT environment. Such a section might cover such topics as the protection of authentication data used by a particular identification and authentication mechanism (e.g. passwords), as well as specific administrative requirements (e.g., investigative procedures needed in response to various intrusion-detection alarms). (268)

Providing a clear identification of known security requirements for the non-IT environment in the PP or ST will help ensure that these security requirements will reliably propagate into user documentation - assuming that the appropriate documentation requirements from Class AGD are included in the PP or ST. (269)

7 The TOE Summary Specification

7.1 Introduction

This chapter provides guidance on the specification of the TOE Summary Specification in an ST (there being no equivalent section in a PP). (270)

[15408-1] subclause C.2.7 requires the following to be included in a TOE Summary Specification: (271)

a) a definition of the IT security functions which satisfy the identified SFRs;

b) optionally, references to security mechanisms or techniques used to implement the IT security functions;

c) a definition of assurance measures which satisfy the identified assurance requirements.

The main parts of the TOE Summary Specification are illustrated in Figure 5 below. (272)

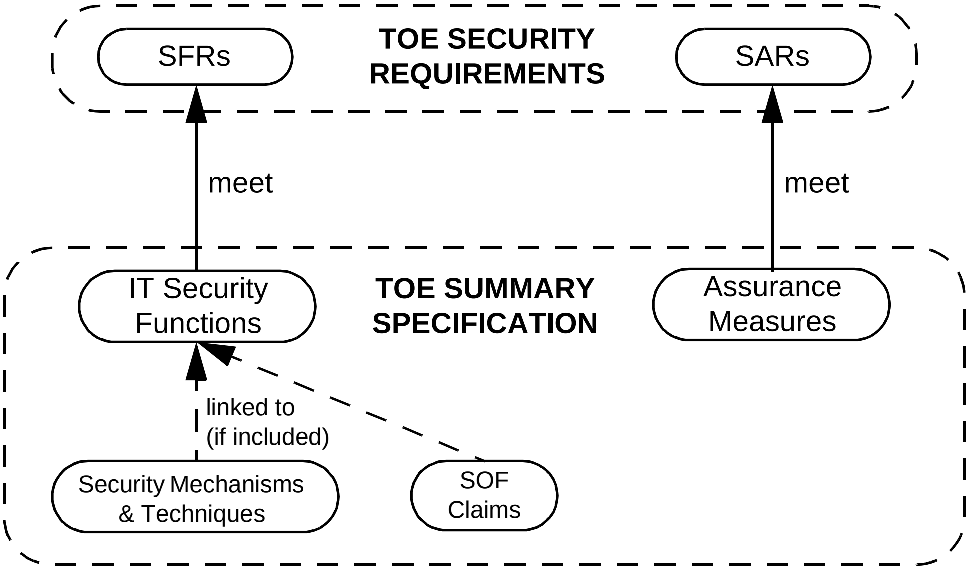

Figure 5 - TOE Summary Specification Content

The main purpose of this section in an ST is to specify the TOE-specific solution to the identified security needs, showing how the TOE provides the security functions and assurance measures to satisfy the defined TOE security requirements. The TOE Summary Specification should therefore be written from this perspective, i.e. defining what the TOE will provide to satisfy the TOE security requirements and thereby meet the security needs. (273)

This section also presents the ST author with the opportunity of organising and specifying the IT security functions in a way that makes the TOE security functionality easier for a reader of the ST to understand, as compared with the SFRs. In particular: (274)

a) The IT security functions may be organised so as to emphasise what the TOE actually does to address the security needs. (By contrast, the SFRs may give a misleading emphasis on supporting functionality, and security management in particular.)

b) The IT security functions may be specified in such a way as to more closely reflect the TOE documentation, for example making appropriate use of TOE-specific terminology. This may improve the cost-effectiveness of the TOE evaluation by providing a more suitable baseline for evaluation than the SFRs, i.e. facilitating clearer mappings from the ST to the TSF representations (e.g. design documentation) and to the developer's test plans and specifications. One possible approach might be to specify a single IT security function to meet a number of SFRs, if it is known that those SFRs are satisfied by the same underlying mechanisms in the TOE design and implementation. This would have the benefit of reducing the amount of representation correspondence evidence the developer needs to provide, without any loss of rigour. The ST author should, nevertheless, ensure that the IT security functions can still be readily traced back to the SFRs they meet.

c) TOE-specific terminology may be included so as (for example) to make the IT security functions more easy to relate to the design or the user or administrator manuals. This may include elaboration of generic terms such as *subject*, *object* or administrator roles.

The TOE Summary Specification may therefore be characterised as a *TOE-specific elaboration of the security requirements the TOE is to meet*. It is *not* necessary to provide details of the TOE implementation, its architecture or its design principles, or to describe in detail how (for example) the developer performs security functional testing of the TOE. (275)

7.2 How to Specify the IT Security Functions

As stated above, ISO/IEC 15408 requires the TOE summary specification in an ST to include a specification of the IT security functions provided by the TOE. The ST must demonstrate that the IT security functions cover all SFRs, and that each IT security function is mapped onto at least one SFR. (276)

Those IT security functions which specify the principal security purpose of the TOE should receive the most detailed attention. In the case of IT security functions corresponding to *supporting* SFRs, you may decide not to include any significant additional detail in the corresponding IT security function; indeed in some cases the IT security function could be defined as identical to the corresponding SFR. Nonetheless, you should still take the opportunity to clarify the functionality where appropriate, for example by using TOE-specific terminology.(277)

The IT security functions may (if appropriate) be organised and labelled differently from the corresponding SFRs, for example in order to simplify the specification of functionality, and to make the corresponding evaluation easier (especially if this facilities the demonstration of traceability to development representations and test evidence). For example: (278)

a) an IT security function may map onto more than one SFR (this may be appropriate for supporting functions); or

b) an SFR may map onto more than one IT security function (this may be appropriate for those functions which directly satisfy the principal security purpose of the TOE).

In performing this reorganisation, you should ensure that: (279)

a) you do not lose essential detail from the SFRs;

b) it does not result in an overly complex mapping of SFRs to IT security functions, increasing the cost of reviewing and evaluating the ST as well as increasing the likelihood of errors.

7.3 How to Specify Security Mechanisms

ISO/IEC 15408 requires the TOE summary specification to provide traceability of IT security functions to any security mechanisms or techniques referenced by the ST. Typical security mechanisms or techniques referenced include encryption and password generation algorithms, or claims of conformance to a relevant ISO or national/government standard. (280)

It should be noted that such references are optional in an ST. In general, it will only be necessary to reference security mechanisms: (281)

a) in the case of a system, where there is a particular requirement to use a specific security mechanism;

b) in the case of a product, where the sponsor sees value in claiming the implementation of specific security mechanisms (or a market demand for such mechanisms or techniques).

7.4 How to Specify the Assurance Measures

ISO/IEC 15408 requires the TOE summary specification to trace assurance measures to assurance requirements, so that it is demonstrated that all assurance requirements are satisfied. ISO/IEC 15408 states that the definition of assurance measures may be made by reference to relevant quality plans, life cycle plans or management plans ([15408-1], subclause C.2.7, page 48). (282)

In practice, it is likely that, for lower assurance levels, this section of an ST will provide little additional information beyond general assertions to the effect that appropriate assurance measures are (or will be) employed to satisfy the security assurance requirements. One recommended approach is to provide a general mapping from the documentation or evidence the developer intends to provide to the appropriate assurance requirements. (283)

At higher levels of assurance (e.g. at EAL5 and above), it may be possible to provide more detail, for example by referencing specific tools, techniques or approaches that the developer has or will adopt to meet the assurance requirements, such as: (284)

a) formal notations to be used in required formal specifications;

b) specific design methodologies or life-cycle models used;

c) configuration management tools;

d) test coverage analysis tools;

e) covert channel analysis methods.

8 PP Rationale

8.1 Introduction

This chapter provides guidance on how to construct a PP rationale. (285)

The purpose of the PP rationale is to demonstrate that a conformant TOE would provide an effective set of IT security countermeasures within the TOE security environment. In particular, it shows that the IT security requirements are suitable to meet the security objectives, which in turn are shown to be suitable to cover all aspects of the TOE security environment (which defines the security needs). The PP rationale is likely to be of most interest to a PP evaluator, although it may aid the understanding of any reader of the PP. (286)

Figure 6 illustrates the key aspects of the PP rationale. (287)

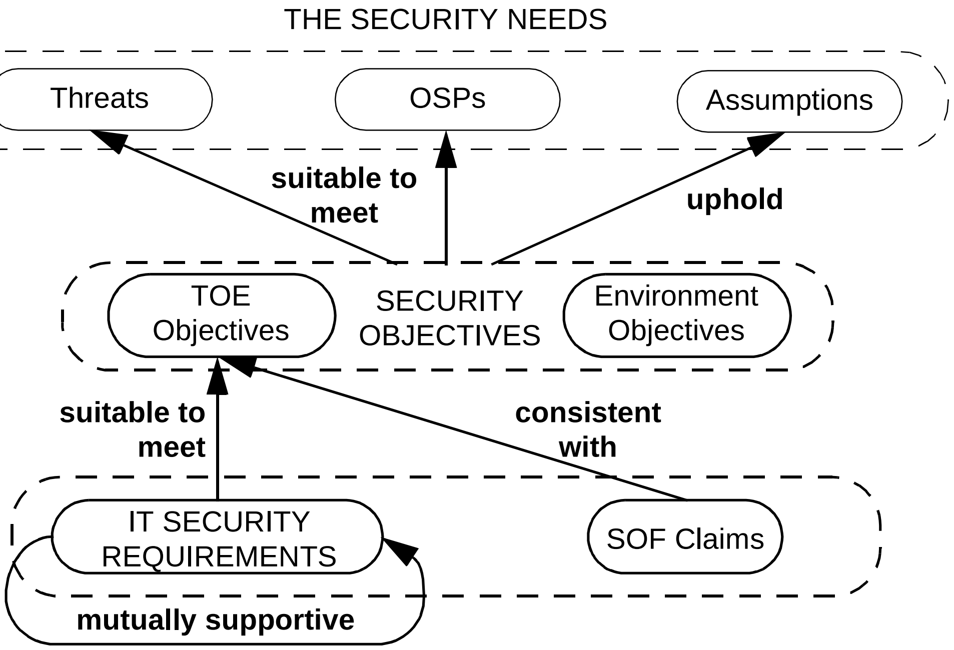

Figure 6 - PP Rationale Requirements

Additionally, the PP rationale must show that: (288)

a) the statement of TOE security assurance requirements is appropriate (APE_REQ.1.4C);

b) unsatisfied dependencies of ISO/IEC 15408 security requirements included in the PP are not necessary (APE_REQ.1.9C).

It is recommended that the requirement to identify completed operations on SFRs (APE_REQ.1.6C) is satisfied within the specification of SFRs rather than as part of the PP rationale. The principal advantage of this approach is that it avoids having to repeat the SFRs in the PP rationale, and thus reduces the likelihood of inconsistencies between the PP and its rationale. (289)

8.2 How to Present the Security Objectives Rationale in a PP

This part of the PP rationale demonstrates that the identified security objectives are suitable, covering all aspects of the security needs as specified in the *TOE Security Environment* section of the PP. This entails showing not only that the security objectives are *sufficient* to address the security needs, but also that they are *necessary*. The following approach is recommended, although alternative approaches may serve equally well. (290)

Firstly, you should include a table which cross-references the threats, OSPs and assumptions against the security objectives which are intended to address them. It should be evident from this table (by inspection of its rows and columns) that: (291)

a) each security objective covers at least one threat, OSP or assumption;

b) each threat, OSP and assumption is covered by at least one security objective.

Satisfying the first condition will be sufficient to demonstrate (for the purposes of the rationale) that each security objective is *necessary* (in other words, there are no obviously redundant security objectives[1]). (292)

Secondly, you need to demonstrate that the security objectives are *sufficient* to meet the security needs, by providing informal arguments to supplement the table. You should organise these arguments around the individual aspects of the TOE security environment that the security objectives need to cover, as follows: (293)

a) For each threat, you should give informal arguments as to why the identified security objectives will provide for effective countermeasures to the threats, i.e. that the security objectives indicate that the event identified in the threat specification can either be:

- detected and recovered from (or damage to assets limited), or
- prevented (or the likelihood of it occurring is reduced to an acceptable level).

b) Similarly, for each identified OSP or assumption, you should give informal arguments as to why the identified security objectives are sufficient either to provide complete coverage of the OSP, or to uphold the assumption.

It is likely that the arguments will focus on the threats and OSPs to be addressed by the security objectives for the TOE. These arguments should: (294)

a) discuss the role of each security objective which is identified as contributing in some way in addressing the threat or satisfying the OSP;

[1] Of course, this does not guarantee that there are no superfluous security objectives, since other security objectives may adequately address the threat or OSP. Whilst you should of course avoid the inclusion of unnecessary security objectives, you do not need to provide any more detailed justification of necessity than this. This determination can be left to the PP evaluator.

b) describe how any relevant environmental security objectives support the security objectives for the TOE in achieving these aims.

This section only justifies the security objectives against the security environment and need not be represented as a full blown risk analysis, even though it contains statements that might be similar to statements in a risk analysis. It is up to the individual organisation to define what is acceptable risk and to complete a risk analysis when revising or defining their security policy. Upon a favourable evaluation the PP or ST, a consumer/user might choose to use this section as a basis for argument in the organisation's risk analysis process. (295)

8.3 How to Present The Security Requirements Rationale in a PP

8.3.1 How to show the security requirements are suitable

The purpose of this part of the PP rationale is to show that the identified IT security requirements (and the SFRs in particular) are suitable to meet the identified security objectives, and thereby address the security needs. As with the security objectives, you need to demonstrate that the IT security requirements are both *necessary* and *sufficient*. The following approach is recommended, although alternative approaches may serve equally well. (296)

Firstly, you should include a table cross-referencing each security objective for the TOE against the SFR which satisfies it. It should be evident from this table (by inspection of the individual rows and columns) that: (297)

a) each SFR addresses at least one security objective;

b) each security objective for the TOE is addressed by at least one SFR.

The latter will be sufficient (for the purposes of the rationale) to demonstrate that each SFR is *necessary* (in other words, there are no obviously redundant SFRs). (298)

Secondly, you should supplement the table with informal arguments for the *sufficiency* of the SFRs. These arguments should be organised around the security objectives for the TOE. For each such security objective, you should provide informal arguments as to why the identified SFRs are sufficient to satisfy the security objective, given that the explicit security requirements and inferred environmental security requirements are satisfied. These arguments should cover all SFRs included in the PP (by functional component), both those which directly satisfy the security objective, and those which play a supporting role (i.e. the *principal* and *supporting* SFRs of section 6.2.1). In constructing the arguments, due consideration should be given to: (299)

a) how and why ISO/IEC 15408 operations have been applied;

b) how TOE security requirements are coordinated with security requirements for the IT environment.

Whilst not mandated by ISO/IEC 15408, the arguments for the sufficiency of the SFRs may also need to discuss the role of any security requirements for the non-IT environment included in the PP (see section 6.5.2). (300)

The following section describes how to show that the SARs are suitable. (301)

8.3.2 How to show the assurance requirements are appropriate

This part of the PP rationale is required to show that the assurance requirements are appropriate for the TOE. This argument should provide a justification as to why the set of SARs is: (302)

a) sufficient to address the security objectives and thus meet the security needs, e.g. if the TOE is intended to defend against attackers who have a high attack potential (as is evident from the threats and security objectives) it would clearly be inappropriate to base the assurance requirements on EAL1, since the evaluation will not consider give due consideration to the vulnerabilities that may be exploited by such attackers (specifically, EAL1 contains no AVA_VLA or AVA_SOF requirements);

b) not excessive, given the statement of security objectives and the security needs;

c) attainable, i.e. that it is technically feasible for this type of TOE to achieve the defined assurance requirements (considerations of cost and timescales are purely a matter for the sponsor of the TOE evaluation).

8.3.3 How to show the strength of function claims are appropriate

ISO/IEC 15408 requires the PP rationale is required to show that the minimum strength of function claim, together with any explicit strength of function claim, is consistent with the identified security objectives. In practice, this means that an argument should be constructed which takes into account: (303)

a) any explicit or implicit strength requirements evident in the stated security objectives for the TOE;

b) any statements made about the technical expertise, resources or motivation of attackers in the security objectives or in the statement of security environment (which defines the security needs which the security objectives are intended to address).

It is possible that such arguments have already been provided as part of the justification of the suitability of the security requirements, in which case they do not need to be repeated. (304)

It should be noted (as pointed out in [15408-1], subclause B.2.6, page 40) that this requirement is only applicable if the SARs include AVA_SOF.1. This, of course, presumes that if the SARs omit AVA_SOF.1, this does not undermine the suitability of the security requirements to meet the security objectives (as discussed in preceding sections). (305)

8.3.4 How to show the security requirements are mutually supportive

The purpose of this part of the PP rationale is to show that the IT security requirements (and the SFRs in particular) are complete and internally consistent by demonstrating that they are mutually supportive and provide an ‘integrated and effective whole’. The following approach is recommended: (306)

a) demonstrate that functional and assurance component dependencies are satisfied where necessary;

b) provide an argument for internal consistency between the IT security requirements;

c) show that supporting SFRs have been included where appropriate to defend other SFRs against attacks such as bypassing or tampering.

Each of these aspects of mutual support is now dealt with in turn. (307)

Component dependency analysis

This analysis can be most effectively presented by means of a table or tree diagram (these being more clear and concise methods than that of providing a textual justification). If the SARs are based purely on an ISO/IEC 15408 EAL or other assurance package, the analysis should only to cover the dependencies of the SFRs (since assurance packages will normally be self-contained, with all dependencies satisfied). (308)

Whatever method is chosen, it should be capable of: (309)

a) demonstrating where dependencies are satisfied *at the level of the SFRs*, i.e. for each iteration of a functional component;

b) identifying any unsatisfied dependencies, and providing an explanation as to why each such dependency does not need to be satisfied.

The reason for performing the dependency analysis at the level of the SFRs is that if a component is iterated a number of times, then it may also be necessary to iterate those components on which it depends. For example, FMT_MSA.3 (Static Attribute Initialisation) is dependent on FMT_MSA.1 (Management of Security Attributes). If FMT_MSA.3 is iterated to cover the initialisation of a number of different security attributes, it is quite likely that it will be necessary to iterate FMT_MSA.1 the same number of times to cover the management of each of these attributes. In this event, a dependency analysis which claimed that the dependency of FMT_MSA.3 was satisfied purely because the functional component FMT_MSA.1 was included in the PP would be incomplete (and potentially misleading), since the FMT_MSA.1 SFRs might not actually cover all of the security attributes referenced by the FMT_MSA.3 SFRs. (310)

A dependency may not need to be satisfied because (for example) it may be irrelevant to the TOE, or it may be unnecessary given the statement of security objectives. Alternatively, the dependency may be satisfied by the IT environment, or by non-IT means. (311)

One possible approach to presenting the dependency analysis is to construct a table which: (312)

a) includes one row for each functional component included in the PP, with multiple rows for multiple occurrences of a component;

b) assigns a unique label or number to each such row (so that each individual SFR is uniquely identified);

c) identifies the functional component associated with each row;

d) lists, for each functional component identified, the dependencies on other components as defined in [15408-2];

e) provides, for each dependency that is identified, either the reference label or number of the row which satisfies the dependency *or* an explanation as to why the dependency does not need to be satisfied.

The demonstration in respect of assurance dependencies should be relatively straightfoward. If the PP simply mandates a ISO/IEC 15408 EAL or assurance package, then the PP rationale may simply assert that all assurance-assurance dependencies are satisfied because of this. If the PP includes augmented assurance requirements, then the PP rationale must show that any additional dependencies introduced are satisfied. (313)

[15408-2] identifies a small number of functional-assurance dependencies. These can be shown to be satisfied in the table described above. For example, if the PP mandates FPT_RCV.1, which has a dependency on AGD_ADM.1, and the target evaluation assurance level is EAL4, then the table entry for this dependency should be ‘EAL4’ instead of an SFR reference. (314)

This dependency analysis will go some way to demonstrating that the IT security requirements are mutually supportive. In other words, if functional component A is dependent on functional component B, then by definition B is supportive of A. (315)

Internal consistency

For the second aspect of the demonstration of mutual support, you need to provide an argument for the internal consistency of the IT security requirements (this being a pre-requisite to mutual support), given that all component dependencies have been shown to have been satisfied where relevant. In the case of SFRs, this can be done by considering where different SFRs apply to the same types of events, operations or data. For example, if the PP includes requirements for the individual accountability of users as well as requirements for user anonymity, it needs to be shown that these requirements do not conflict. This might involve showing that none of the auditable events requiring individual user accountability relate to operations for which user anonymity is required. (316)

Defence of SFRs against attack

The other forms of support that you need to consider in this part of the PP rationale are relevant only to the SFRs. This is because demonstration of mutual support involving assurance requirements is trivial: (317)

a) By definition, SARs support the SFRs, since they provide confidence that the functional requirements are met.

b) Whilst SFRs and SARs are mutually supportive in a general sense, there are few *specific* instances of SFRs which provide support to specific SARs that would merit discussion in a PP rationale. However, one typical example would be that of FPT_SEP (Domain Separation) components, which support ADV_HLD (High-level Design) components by helping to achieve separation.

c) SARs may be asserted to be mutually supportive provided the dependencies are satisfied.

As described in section 6.2.1, *supporting* SFRs may help defend *primary* SFRs against attacks aimed at defeating those SFRs, where the ulterior motive of the attacker is to subsequently mount one or more of the threats that the *primary* SFRs are intended to counter. Mutual support encompasses both this kind of support as well as the kind associated with ISO/IEC 15408 security requirements dependencies. (318)

Consideration of mutual support between SFRs not addressed by the dependency analysis should address those SFRs which: (319)

a) help prevent the bypassing of other SFRs;

b) help prevent tampering with other SFRs (including any security attributes or other data the integrity of which is essential to the SFR);

c) help prevent de-activation of other SFRs;

d) enable the detection of the misconfiguration of another SFR, or of attack aimed at defeating another SFR.

Bypass of an SFR is typically defended against by FPT_RVM.1 (Non-bypassability of the TSP). Where the enforcement of security by an SFR is dependent on the TOE knowing the identity of the interacting user (e.g. access control), then user authentication requirements (using components from the FIA_UAU family) will also prevent bypass of those SFRs (by impersonation of a different user). It should, however, be noted that not all SFRs will require support from other SFRs to prevent bypass; this will be the case where: (320)

a) the decision as to whether to invoke the function rests not with the TSF, but with a user or administrator, e.g. SFRs based on FDP_DAU (Data Authentication) components;

b) the wording of the SFR stipulates that the function is always invoked when necessary, and hence the SFR cannot be bypassed if the SFR is satisfied by the TSF, e.g. as is the case with SFRs based on FDP_RIP (Residual Information Protection) components.

Tampering attacks are relevant to all SFRs. Such attacks may be defended against by: (321)

a) FPT_SEP (Domain Separation) components, which prevent external interference or tampering by untrusted subjects;

b) FTP_PHP (TSF Physical Protection) components, which provide the means to detect or resist physical tampering attacks;

c) SFRs based on security management components such as FMT_MSA.1 (Management of Security Attributes), which restrict the ability to modify security attributes or configuration data;

d) SFRs based on components such as FMT_MTD.1 (Management of TSF Data) or FAU_STG.1 (Protected Audit Trail Storage), which protect the integrity of security critical data;

e) FTP_TRP (Trusted Path) components, which prevent tampering attacks based on spoofing of the TSF (e.g. by a password-grabbing program).

De-activation may not be relevant to all SFRs as specified in the PP. However, one example where de-activation *is* relevant is security audit; the FAU_STG (Security Audit Event Storage) family includes requirements to prevent the de-activation of the security audit functions arising as a result of the audit trail filling. SFRs specified using FMT_MOF.1 (Management of Security Functions Behaviour) may also help prevent de-activation of some security functions. (322)

Detection functions such as security audit provide support to other SFRs by providing the ability to detect possible attack aimed at defeating particular SFRs, or potential misconfiguration which could leave the TOE prone to attack. Other detection functions include components from the FDP_SDI (Stored Data Integrity) and FPT_PHP (TSF Physical Protection) families. (323)

9 ST Rationale

9.1 Introduction

This chapter provides guidance on how to construct an ST rationale. The purpose of the ST rationale is to demonstrate that all aspects of the identified security needs (as defined in the TOE security environment) are suitably addressed by the security objectives, and that the security objectives for the TOE are suitably met by the identified IT security requirements, which in turn are suitably met by the IT security functions and assurance measures. The ST rationale is therefore similar to a PP rationale, but additionally provides a justification of the contents of the TOE summary specification, showing that it is suitable to meet the TOE security requirements. (324)

As with a PP rationale, the ST rationale is likely to be of most interest to an ST evaluator, although the content of the rationale may be helpful to other readers of the ST. (325)

Figure 7 illustrates the key ST-specific aspects of the ST rationale. (326)

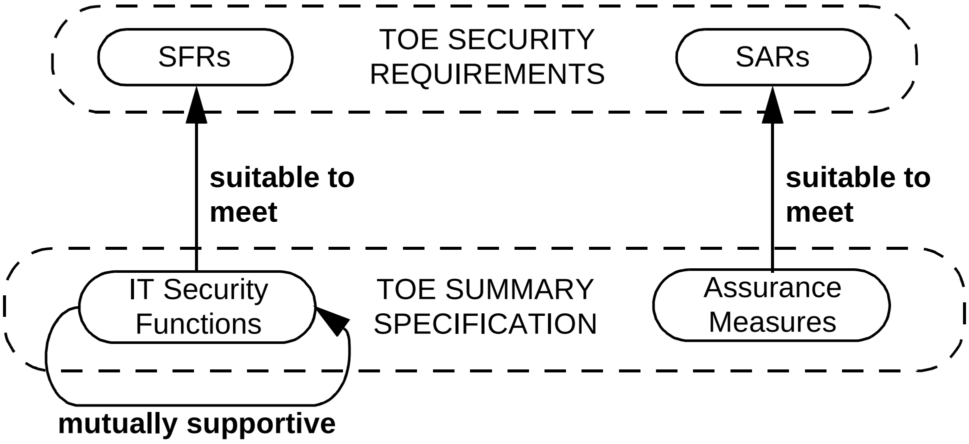

Figure 7 - ST-Specific Aspects of Rationale

(327)

Additionally, the ST rationale must demonstrate that any claim of compliance with a PP is justified (in accordance with ASE_PPC.1). (328)

The guidance in this chapter assumes that the ST claims compliance with one or more PPs, and therefore that the PP rationale is ‘inherited’ by the ST. This means that the ST rationale needs only to focus on those aspects that are not included within the PP. Should the ST not claim compliance with any PP, then a full rationale must be provided as described in the previous chapter (sections 8.2 and 8.3). (329)

9.2 How to Present The Security Objectives Rationale in an ST

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.2). If the ST claims compliance with a PP, then this part of the ST rationale should simply address any differences from the PP, showing: (330)

a) that any additional threats are addressed by the security objectives;

b) that any additional OSPs are met by the security objectives;

c) how any additional security objectives address the relevant threats and/or OSPs.

9.3 How to Present the Security Requirements Rationale in an ST

9.3.1 How to show the security requirements are suitable

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.3.1). If the ST claims compliance with a PP, then this part of the ST rationale should simply address any differences from the PP, showing: (331)

a) that any additional security objectives for the TOE are met by the SFRs;

b) how any additional SFRs address the relevant security objectives.

9.3.2 How to show the assurance requirements are appropriate

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.3.2). If the ST claims compliance with a PP, but specifies augmented assurance requirements, then the additional requirements should be justified as being appropriate. The ST rationale should also take into account any differences in the TOE security environment or security objectives. (332)

9.3.3 How to show the strength of function claims are appropriate

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.3.3). (333)

9.3.4 How to show the security requirement dependencies are satisfied

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.3.4). If the ST claims compliance with a PP, then this part of the ST rationale should simply address any differences from the PP, i.e. showing that dependencies are satisfied for all additional SFRs and assurance requirements. (334)

9.3.5 How to show the security requirements are mutually supportive

This part of the ST rationale should be constructed as described in the previous chapter for the PP rationale (see section 8.3.4). If the ST claims compliance with a PP, then this part of the ST rationale should simply address any differences from the PP, showing how any additional security requirements: (335)

a) are supported by other IT security requirements;

b) provide support to other IT security requirements;

c) are consistent (do not conflict) with other IT security requirements.

9.3.6 How to show the ST complies with the referenced PPs

This part of the ST rationale is required to identify the PPs to which the ST is claimed to comply, and show that: (336)

a) all PP security objectives are included, and any refinements of the security objectives are valid;

b) all PP security requirements are included, and any refinements or other operations on PP security requirements are valid;

c) no IT security requirement conflicts with any PP security requirement[1].

Where the ST includes the PP security objectives and security requirements verbatim (or references them), and includes no additional security objectives or requirements, then no further analysis is required. Further analysis is only necessary where the ST includes additional details. Any such details must be justified by showing that these do not conflict with anything stated in the PP. (337)

Additionally, where the PP includes incomplete operations on security requirements, leaving assignment or selections to the ST author, it must be evident from the ST that all such operations are completed. (338)

9.3.7 How to show the IT security functions satisfy the SFRs

The purpose of this part of the ST rationale is to provide a demonstration that the specified IT security functions are suitable to meet all SFRs included in the ST (and not just those SFRs that feature in any referenced PP). The recommended approach is to demonstrate the mapping of the IT security functions onto the SFRs by means of a table. The table should show that: (339)

a) each SFR is mapped onto at least one IT security function;

b) each IT security function is mapped onto at least one SFR.

In addition to the table, an explanation should be given wherever it is not self-evident how a particular SFR is satisfied. This may be necessary, for example, where there are many IT security functions mapping onto a single SFR. (340)

9.3.8 How to show the IT security functions are mutually supportive

The purpose of this part of the ST rationale is to show that the IT security functions are complete and internally consistent by demonstrating that they are mutually supportive and provide an ‘integrated and effective whole’. (341)

[1] Conflict between additional IT security requirements should, of course, be addressed when demonstrating that the IT security requirements as a whole are mutual supportive.

This analysis should be performed in much the same way as that described for the demonstration of mutual support between the SFRs. Since mutual support will already have been demonstrated for the SFRs, this part of the analysis should focus on the impact of any additional detail introduced in the specification of the IT security functions as compared with the corresponding SFRs. Any instances of support or interrelations between IT security functions that are introduced as a result of the inclusion of this additional detail should be discussed. Nonetheless, since the TOE summary specification is (in effect) a re-expression of the SFRs from the perspective of the TOE, any reuse of the results of the analysis of the SFRs should interpret the results from this different perspective. (342)

9.3.9 How to show the assurance measures satisfy the assurance requirements

The purpose of this part of the ST rationale is to show that the identified assurance measures are appropriate to meet the assurance requirements. The recommended approach is to provide a mapping of the identified assurance measures onto the assurance requirements, demonstrating that each assurance requirement is addressed. Where specific assurance measures are identified (see section 7.4), this mapping may be best presented in tabular form. This should be accompanied by a brief explanation of how the assurance requirements will be satisfied. It should be noted, however, that the assessment of the suitability of the assurance measures cannot prejudge the evaluation of the TOE, which will provide the only concrete proof of whether the chosen assurance measures are appropriate. Therefore a detailed justification of suitability is not expected in the ST. (343)

In practice, it is likely that most attention will be paid to this part of the ST rationale where the ST includes SARs that require the use of specific high-assurance techniques (e.g. covert channel analysis or the use of formal methods). (344)

10 PPs and STs for Composite and Component TOEs

10.1 Introduction

This chapter provides guidance related to the specific issues raised by the notion of composability, addressing the following cases: (345)

a) where a PP or ST is being written for a *composite TOE*, that is a TOE that is composed of two or more components (which may themselves be *composite TOE*s), each of which has its own individual PP or ST (termed *component TOE PP* or *component TOE ST* within this Guide);

b) where a PP or ST is being written for a *component TOE* that has identified dependencies on the IT environment, which includes other component TOEs that are part of a composite TOE (note there may also be dependencies on security requirements for the non-IT environment, but these are not required to be a formal part of a PP or ST).

A number of possible scenarios exist, for example: (346)

a) A composite TOE ST may be written where the identities of the component TOEs are already known, and where the STs for these component TOEs already exist. The principal purpose of the composite TOE ST will thus be to define the security needs to be met by the component TOEs as a whole, and to demonstrate that all aspects are addressed.

b) A composite TOE PP may be written with a view to decomposing the problem into individual component TOEs, and then writing PPs for those individual components. The principal purpose of the composite TOE PP is as described above. Component TOE STs will therefore need to be matched against the security requirements of the component TOE PPs.

This general approach will be particularly appropriate for large system architectures that contain many components. The choice of how to best decompose the composite TOE for the purposes of writing component TOE PPs or STs is a matter for the composite TOE PP/ST author to decide.(347)

It should be noted that, to date, there has been little practical experience in the area of composability. Further guidance will be provided in future versions of the Guide as and when further practical experience is gained in this area. (348)

10.2 The Composite TOE

10.2.1 Descriptive parts of the PP and ST

The descriptive parts of the component TOE PP/ST, and the TOE description in particular, should describe the composite TOE, identifying the various components of the TOE. The *TOE Description* sections in the component TOE PPs or STs should be referenced for a description of the TOE functionality; this information should be summarised in the composite TOE PP/ST. (349)

10.2.2 TOE Security Environment

The *TOE Security Environment* section in a PP or ST for a *composite TOE* may either: (350)

a) specify the security environment for the composite TOE in full (or by reference to one of more PPs with which conformance is claimed, with additional details included where appropriate); or

b) provide a general description of the security needs (to give the reader an overall picture), referencing the component TOE PPs or STs for the detailed definition of the threats, OSPs and assumptions.

The first approach may be appropriate where a composite TOE PP is being written first, and there is known to be a significant degree of uniformity across the component TOEs in terms of the assets to be protected and the threats to those assets. In this case, the component TOE PPs would simply reference the definition of the TOE security environment rather than repeating the information. (351)

The second approach may be more appropriate if the component TOE PPs or STs already exist. It is also likely to be appropriate if there are many different assets to be protected, each of which is only relevant to a limited subset of the components of the composite TOE. In such an event, a full description in the composite TOE PP/ST would be likely to be over-complex and thus difficult for the reader to understand. A general description of such things as assets and threat agents is therefore likely to be more helpful to the reader, providing a context for the definition of the security needs provided in the individual component TOE PPs or STs. (352)

It should be noted that ISO/IEC 15408 points out that where a TOE is physically distributed, it may be necessary (for the purposes of clarity) to identify the distinct domains of the TOE security environment, and discuss the security environmental aspects (threats, OSPs and assumptions) separately for these. (353)

Whichever approach is taken, you need to ensure that there is consistency between the composite TOE PP/ST and the component TOE PPs/STs. (354)

10.2.3 Security Objectives

The statement of security objectives should be provided in the component PPs or STs, and should not need to be restated in full in the PP/ST for the composite TOE. However, it may be appropriate to summarise the information in the composite TOE PP/ST, showing which components satisfy which security objectives. (355)

If, however, security objectives have been identified in the composite TOE ST that are not exactly the same as those in the STs for the individual component TOE, then you should provide a mapping from the composite TOE security objectives to those of the component TOEs. (356)

10.2.4 Security Requirements

The statement of IT security requirements should be provided in the component TOE PPs or STs, and does not need to be restated in full in the PP/ST for the composite TOE. However, it may be appropriate to summarise the information in the composite TOE PP/ST, by mapping SFRs onto components and identifying the level of assurance in those SFRs. (357)

An exception to this is where a uniform level of assurance has been identified for the composite TOE. In this case, it may be appropriate to specify the assurance requirements in one place (the composite TOE PP/ST), with the component TOE PPs/STs referring to this definition of requirements. (358)

It may be noted that it is possible for a composite TOE PP/ST to specify an ‘assurance profile’ such that SFRs provided by different component TOEs have different assurance requirements. This may be appropriate, for example, where a component TOE is selected to protect assets of a particularly high value, or which are particularly attractive to an attacker. Such an approach is not expressly forbidden by ISO/IEC 15408, but you must ensure that you do not end up with a profile in which SFRs provided by one component TOE are dependent on SFRs provided by another component TOE that is to be evaluated to a lower level of assurance. (359)

Note that in the case of a composite TOE PP or ST that specifies an assurance profile, the identification of an overall assurance level has no meaning, except to the extent that a *minimum* assurance level can be identified. (360)

Pragmatic considerations in the design of large multiple component systems demand that high-assurance component TOEs be minimised, due to the increased cost of development and evaluation. The general philosophy is to isolate the assets that need the most protection into a small number of high-assurance component TOEs (e.g. isolate the root keys held by a certification authority). (361)

When writing a composite TOE PP/ST, you will need to ensure that all dependencies of all component TOEs are satisfied by other component TOEs, unless of course it is intended that the composite TOE is itself to form a component of a larger TOE. The IT Security Requirements section of the composite TOE PP/ST should therefore identify any unsatisfied dependencies that are to be satisfied by the IT environment for the composite TOE (if such a thing exists). (362)

10.2.5 TOE Summary Specification

A composite TOE ST should reference the TOE summary specifications of the component TOE STs rather than repeat the detail. The *IT Security Requirements* section of the composite TOE ST should already identify which component TOEs satisfy which IT security requirements, and therefore there will be little to be gained from attempting to list the IT security functions provided by each component TOE. (363)

If the TOE summary specifications of the component TOE STs identify additional or more detailed dependencies on other component TOEs, it will be necessary for the composite TOE summary specification either to show that these are satisfied for the composite TOE as a whole, or to specify the unsatisfied dependencies as security requirements on the IT environment for the composite TOE. (364)

10.2.6 PP Rationale

A composite TOE PP must show that the set of security objectives is suitable to address all aspects of the TOE security environment, and that the IT security requirements are suitable to meet the security objectives. For some aspects of the PP rationale it will be possible to refer to details in the component TOE PP rationales. The following approach should be adopted: (365)

a) To show that the set of security objectives for the composite TOE as a whole is suitable to address the security needs for the composite TOE, you first need to map each component TOE security objective onto the threats and OSPs specified in the composite TOE PP. You should then provide arguments as to why the security objectives are suitable to counter the threats and meet the OSPs. It will only be possible to reference the PP rationale of individual component TOEs if the composite TOE threats or OSPs precisely map onto those specified in the component TOE PPs.

b) To show that the set of IT security requirements is suitable to meet the security objectives, you should reference the PP rationales for the individual component TOEs where a component TOE satisfies a security objective for the composite TOE. You should, in the composite TOE PP, demonstrate that all security objectives for the composite TOE are suitably met by at least one of the component TOEs, and provide an explanation where two or more component TOEs cooperate to meet a security objective.

c) To show that dependencies of IT security requirements are satisfied, you may reference the PP rationales for the individual component TOEs. However, you should ensure that the PP rationale for the composite TOE:

- demonstrates that all dependencies that are to be satisfied by the IT environment in individual component TOE PPs are either satisfied by other component TOEs within the composite TOE as a whole, or are identified (in the composite TOE PP) as dependencies on the IT environment for the composite TOE;
- considers dependencies that were argued away in the component TOE PP rationales, since these arguments may no longer be valid in the context of the composite TOE security environment.

d) To show that the IT security requirements are mutually supportive, you may reference the PP rationales for the individual component TOEs for an analysis of interrelationships between IT security requirements *within* each component TOE. However, the composite TOE PP rationale should discuss any interrelationships or dependencies between the IT security requirements applying to *different* component TOEs, where these are not fully addressed by the component TOE PP rationales.

10.2.7 ST Rationale

The guidance for constructing an ST rationale for a composite TOE is very similar to that given in section above for composite TOE PP rationales. In particular: (366)

a) To show that the TOE security requirements are suitably met by the IT security functions and assurance measures, you may simply reference the ST rationales for the component TOEs.

b) To show that the IT security functions are mutually supportive, you may reference the component TOE ST rationales for a demonstration of mutual support *within* the individual component TOEs. However, the composite TOE ST rationale should address interrelationships or dependencies between IT security functions in *different* component TOEs, where appropriate.

10.3 The Component TOE

10.3.1 Descriptive parts of the PP and ST

If it is intended that the TOE is to be a component of a composite TOE, the descriptive parts of the PP or ST (in particular the TOE description) should make this clear. If it is intended that the component TOE be part of a *specific* composite TOE where the other component TOEs are known, the TOE description should identify those other component TOEs with which it is to interact (and which will therefore form the IT environment - or part of it - for the component TOE). Otherwise, the TOE description should describe, in generic terms, the types of composite TOEs that might use this component TOE. (It might be noted that, in principle at least, any TOE can be used in a larger composite TOE.) (367)

10.3.2 TOE Security Environment

The purpose of this section of a PP or ST is to define and scope the security needs to be addressed by the component TOE; from an evaluator’s perspective it will also define the scope of the component TOE evaluation. For example, the IT environment for the component TOE may well contain other IT components with which the component TOE is assumed to interact. In such cases the existence of dependencies of the component TOE on its IT environment should be identified as an assumption on the TOE security environment. Such an assumption should avoid implementation details, since these will be specified elsewhere in the PP or ST. (368)

Similarly, an OSP may mandate that the TOE inter-operates with other devices in the IT environment. In this event the PP or ST should include statements to ensure that evaluators can adequately examine the TOE’s capability to inter-operate as mandated. (369)

10.3.3 Security Objectives

Any dependencies on the IT environment should be identified as security objectives for the (IT) environment. (370)

Note that in the case of a component TOE PP, it is possible that a conformant TOE may actually meet one or more security objectives that the PP places on the IT environment. For example, a DBMS may meet a security objective for identification and authentication of its users, whilst the PP assumes that this security objective will be met by the underlying operating system. (371)

If an OSP is included mandating that the TOE inter-operates with other devices in the IT environment, a security objective for the TOE should be included to meet this OSP. (372)

10.3.4 Security Requirements

Security requirements on the IT environment for a component TOE should, where possible, identify the specific component TOEs which are relied upon to meet those security requirements. Note that the security requirements on the IT environment could be defined by requiring conformance with another PP. (373)

10.3.5 TOE Summary Specification

As part of specification of the IT security functions, it may be appropriate to provide a refinement of any security requirements on the IT environment. For example, the TOE may use a specified operating system interface in order to log generated security audit data. If the component TOE is intended to be part of a *specific* composite TOE, any such refined security requirements on the IT environment should be mapped onto specific components of the composite TOE. (374)

10.3.6 PP Rationale

Where the PP specifies security requirements on the IT environment, these requirements must be considered in the PP rationale, which should show: (375)

a) how the security requirements for the IT environment contribute to satisfying the security objectives for the TOE;

b) that any dependencies of the security requirements for the IT environment are satisfied;

c) how the security requirements for the IT environment are mutually supportive, and how they support the IT security requirements.

10.3.7 ST Rationale

Where the ST specifies security requirements on the IT environment, these must be taken into account in the ST rationale, as described in the previous section for the PP rationale. Any additional details concerning such dependencies that are included in the ST should also be considered in the appropriate places of the ST rationale. (376)

11 Functional and Assurance Packages

11.1 Background

The concept of a *package* is introduced in [15408-1], subclause 4.4.2.1, page 26. A package is characterised in the following terms: (377)

a) it is an **intermediate** combination of functional or assurance components;

b) it is intended to be **reusable**, thereby aiding the construction of PPs, STs, or larger packages;

c) it is intended to define security requirements which are **known to be useful** in meeting an identifiable subset of security objectives.

The principal benefit of packages that can be reused in a number of PPs and STs is that they will reduce the cost of PP/ST development by cutting down the workload on PP/ST authors when they come to specify the IT security requirements (see Chapter 6). The guidance in this chapter relating to the construction of packages is therefore intended to support the above aims. (378)

ISO/IEC 15408 does not specify any requirements on functional or assurance packages, although it is possible to apply a suitable subset of the APE assurance requirements to a package. Indeed, it may be helpful to PP/ST authors if the package is structured like a PP, in which sections that are left to be specified by the PP/ST author are clearly identified as such. Issues such as validation and registration of packages are, however, outside the scope of this Guide. (379)

It should be noted that experience in the construction of packages is very limited. Currently, the only widely available examples of packages are the EALs defined in clause 6 of [15408-3], which should be consulted as an example of how an assurance package may be specified. (380)

11.2 How to Specify a Functional Package

11.2.1 Who might write a functional package?

Any organisation wishing to promote the use of a standardised specification of security functionality may choose to produce a functional package. They may do so as a first step towards the production of a PP (or a family of PPs), or they may wish to encourage its use in STs. A functional package could, for example, be used by an organisation to specify a standard set of security functional requirements which product vendors should meet. (381)

11.2.2 What must a functional package contain?

Fundamentally, a functional package is a specification of SFRs. As such, these SFRs should be specified following the guidance given in section 6.2 above. Thus each SFR included in the functional package must either: (382)

a) clearly identify ISO/IEC 15408 Part 2 functional component from which it is drawn, identifying which operations are completed and which are uncompleted; or

b) be identified as explicitly stated without reference to ISO/IEC 15408, with a justification as to why it needed to be explicitly stated; each such SFR must satisfy the criteria expressed in APE_SRE.1.3C-1.5C, i.e. it must:

- use ISO/IEC 15408 requirements components, families and classes as a model for presentation;
- be measurable and state objective evaluation requirements;
- be clearly and unambiguously expressed.

The set of SFRs specified must be known to satisfy an identifiable subset of security objectives. The author of a functional package should therefore either: (383)

a) begin with one or more specified security objectives, and derive a set of SFRs which will meet them; or

b) ‘reverse engineer’ the security objectives from the defined set of SFRs.

In practice, the author of a functional package may adopt some combination of these two approaches. (384)

11.2.3 What *should* a functional package contain in order to be useful?

In order to be useful, a functional package must be *reusable* in a larger functional package, or in a PP or ST. A PP or ST author is likely to find the following information helpful: (385)

a) an identification of the security objectives which the SFRs satisfy;

b) notes on the use of ISO/IEC 15408 Part 2 components, or on the deviation from ISO/IEC 15408 Part 2;

c) rationale for the SFRs, covering:

- the suitability of the SFRs to satisfy the identified security objectives;
- dependency analysis;
- demonstration of mutual support between SFRs.

It is not, however, recommended that a functional package contain a formal specification of security objectives, or a full security requirements rationale which satisfies the relevant assurance criteria expressed in [15408-3]. This is because the security objectives for a particular TOE will be influenced by the statement of TOE security environment, and thus will to some extent be specific to the defined security needs for the TOE. Rather, the functional package should contain, in the form of application notes, any relevant information which could be used by PP or ST authors when in the constructing their PP or ST rationale. (386)

11.3 How to Specify an Assurance Package

11.3.1 Who might write an assurance package?

An evaluation authority may choose to specify assurance packages for use in evaluations under the relevant national scheme. Such packages could be (for example) definitions of alternative assurance levels, or the definition of the combination of components from the AMA *Assurance maintenance* class called up by a national assurance maintenance scheme. Similarly any organisation with a general need for evaluation of the systems they own may choose to define a set of assurance requirements tailored to their specific needs and concerns. (387)

11.3.2 What must an assurance package contain?

Fundamentally, an assurance package is a specification of security assurance requirements. As such, these requirements should be specified following the guidance given in section 6.3. Thus each security assurance requirement included in the assurance package must either: (388)

a) clearly identify ISO/IEC 15408 Part 3 assurance component from which it is drawn; or

b) be identified as explicitly stated without reference to ISO/IEC 15408, with a justification as to why it needed to be explicitly stated; such security requirements satisfy the criteria expressed in APE_SRE.1.3C-1.5C, i.e. it must:

- use ISO/IEC 15408 requirements components, families and classes as a model for presentation;
- be measurable and state objective evaluation requirements;
- be clearly and unambiguously expressed.

11.3.3 What *should* an assurance package contain to be useful?

To support the goal of reusability, an assurance package should contain supporting information which describes the intended objectives of the set of assurance requirements. This information will enable the reader to decide under what circumstances the package should be used, and what (if any) other assurance requirements would be appropriate to combine with it. (389)

The specification of EALs given in [15408-3] clause 6 should be used as a model for the presentation of assurance packages. (390)

Annex A Guidance Checklist

This annex lists the key points from the guidance provided in Chapters 3 to 9 of this Guide. (391)

A.1 PP/ST Introduction

Provide, in the PP/ST Overview, a top-level overview of the security problem being solved by the PP/ST, and how the PP/ST contributes to the solution. (392)

Ensure the PP/ST Overview is consistent with the technical content of the PP/ST. (393)

A.2 TOE Description

Include a general TOE functional description which is not confined to a description of TOE security features (unless the TOE is a special-purpose security product). (394)

Consider including in the TOE description in a PP a description of the TOE boundary, informing the reader what is in the TOE and what is not. (395)

Include in the TOE description in an ST a description of the TOE boundary. (396)

Ensure the TOE description is consistent with the technical content of the PP/ST. (397)

A.3 Defining the Statement of TOE Security Environment

A.3.1 Assumptions

Identification

Include any assumptions you are making about the TOE security environment or the scope of the security needs, relating in particular to physical, personnel, procedural or connectivity aspects of the environment. (398)

Definition

Avoid, where possible, the inclusion of details relating to the TOE security functions in the definition of assumptions. (399)

Presentation

Assign unique labels to environmental assumptions for ease of reference. (400)

A.3.2 Threats

Identification

Identify the threats that are relevant by identifying the IT assets that require protection, what attack methods or other undesirable events they need to be protected from, and who or what are the threat agents. (401)

Definition

Ensure the threat descriptions are *clear* by detailing the source of the threat (or threat agent), the IT assets under attack, and the attack method. (402)

Ensure the threat descriptions are *concise* by minimising overlap between threats. (403)

Only include events which *directly* compromise the IT assets, rather than attacks based on flaws or weaknesses in the TOE implementation. (404)

Presentation

Assign unique labels to threats for ease of reference. (405)

A.3.3 Organisational Security Policies

Identification

Identify as OSPs any security policy requirements that cannot be derived from consideration of the threats alone. (406)

Definition

Define OSPs in the form of a set of rules to be implemented by the TOE and/or its environment (e.g. access control rules). (407)

Presentation

Assign unique labels to OSPs for ease of reference. (408)

A.4 Defining the Security Objectives

Identification

Where the SFRs are already known, identify one security objective for the TOE corresponding to each of the principal SFRs to be satisfied by the TOE, so as to facilitate the mapping from security objectives to SFRs. (409)

Identify any security objectives to be satisfied by the IT environment (e.g. an underlying platform) as the security objectives for the environment. (410)

Identify any procedural responsibilities relating to the management and use of the TOE countermeasures as the security objectives for the environment (411)

Definition

Define security objectives for the TOE as a *concise* statement of the intended response to the identified security needs, indicating the extent to which the needs will be addressed. Don't simply restate threats and OSPs in a different form. Avoid, where possible, reference to implementation details. (412)

Define security objectives for the TOE that counter threats such that it is clear whether they are *preventative, detective*, or *corrective*. (413)

Presentation

Assign unique labels to security objectives for ease of reference. (414)

A.5 Specifying the IT Security Requirements

A.5.1 TOE Security Functional Requirements

Identification

Identify, as a first step, those SFRs that will *directly* satisfy each of the security objectives for the TOE. (415)

Identify the complete set of SFRs by identifying all SFRs that are needed to play a supporting role in achieving the security objectives for the TOE. (416)

Identification of the set of supporting SFRs includes consideration of the relevant functional component dependencies as identified in ISO/IEC 15408 Part 2. Such dependencies do not need to be satisfied if they can be argued as not necessary given the statement of security objectives.(417)

Definition

Select the level of auditing depending on the importance of audit in achieving the security objectives, and technical feasibility. (418)

Use the *iteration* operation where multiple invocation of a given ISO/IEC 15408 Part 2 functional component is necessary. (419)

Complete, or partially complete, *assignment* and *selection* operations on functional components in a PP where it is necessary to preclude the choice of solutions that are inconsistent with the security objectives for the TOE. (420)

Consider the use of the *refinement* operation where substitution of a generic term (e.g. security attribute) for a TOE-specific term would make the SFR more readable and understandable. (421)

Presentation

Use italics (or some other means of highlighting text) to show operations that are completed in a PP or ST. (422)

Group the SFRs under headings that are appropriate for your PP/ST: don’t feel constrained by ISO/IEC 15408 Part 2 class, family or component headings. (423)

Consider adopting a unique SFR labelling scheme specific to your PP/ST: you are not constrained to use ISO/IEC 15408 Part 2 component labelling scheme, provided the SFRs are clearly traced back to the appropriate ISO/IEC 15408 Part 2 functional component. (424)

A.5.2 TOE Security Assurance Requirements

Identification

Select assurance requirements based on the value of assets to be protected, the risk to those assets, technical feasibility, likely costs and timescales. (425)

A.5.3 IT Environment Security Requirements

Identification

Identify security requirements on the IT environment to satisfy any security objectives that are to be met by the IT environment. (426)

Identify supporting security requirements for the IT environment to satisfy any dependencies of the TOE SFRs that are not satisfied by the TOE, and which cannot be argued as not relevant to the security needs. (427)

Definition

Define security requirements on the IT environment at an appropriate level of abstraction: in the case of a PP, defining requirements at the level of the SFRs may in some instances be too implementation-specific. (428)

A.6 Producing the TOE Summary Specification

A.6.1 IT Security Functions

Identification

Identify the IT security functions based initially on the SFRs; organise the IT security functions to make it easy to relate them to the TOE documentation, without introducing undue complexity into the SFR to IT security function mapping. (429)

Definition

Define the IT security functions by incorporating appropriate TOE-specific details, whilst ensuring that none of the essential details contained in the SFRs is lost. (430)

A.6.2 Assurance Measures

Identification

Identify general assurance measures in an ST, ensuring all assurance requirements are covered, where low assurance requirements are defined that require no specialist methods or techniques, e.g. a general statement to the effect that assurance measures will be adopted as appropriate to meet the security assurance requirements. (431)

Identify specific detailed assurance measures in an ST where high assurance requirements are included requiring specialist methods or techniques. (432)

A.7 Constructing the PP Rationale

A.7.1 Security Objectives Rationale

Demonstrate the mapping of security objectives to threats, organisational security policies and assumptions by means of a table (or other suitable method) showing that each threat, OSP and assumption is addressed by at least one security objective. (433)

For each threat, OSP and assumption, supplement this with an argument as to why the identified security objectives are suitable to cover them. (434)

A.7.2 Security Requirements Rationale

Demonstrate the SFR to security objective mapping by means of a table (or other suitable method) showing that each security objective for the TOE is addressed by at least one SFR. (435)

For each security objective for the TOE, supplement this with an argument as to why the identified security requirements are suitable to meet them. (436)

Demonstrate mutual support by showing that ISO/IEC 15408 component dependencies are satisfied where appropriate and that the SFRs do not conflict, and by highlighting any additional supportive dependencies between SFRs, e.g. SFRs which prevent other SFRs from being bypassed, tampered with or de-activated. (437)

A.8 Constructing the ST Rationale

A.8.1 Security Objectives and Security Requirements Rationale

Present these parts of the ST rationale by following the guidance given in section A.7 above. Where conformance is claimed with a PP, the ST rationale should focus on the impact of any additional details introduced into the ST security objectives and IT security requirements. (438)

A.8.2 TOE Summary Specification Rationale

Demonstrate the mapping of IT security functions to SFRs, and assurance measures to SARs, by means of a table (or other suitable method) showing that each SFR and SAR is addressed by at least one IT security function or assurance measure, as appropriate. (439)

Annex B Generic Examples

This annex provides lists of example threats, organisational security policies, assumptions and security objectives, presented in a form that could be used in a PP or ST. It also provides guidance relating to ISO/IEC 15408 Part 2 functional components that may be used for specifying common or generic security functional requirements. (440)

The intention here is to illustrate a style of specification and naming convention for threats, OSPs, assumptions and security objectives, with a view to promoting consistency amongst PPs and STs, which will in turn facilitate comparison between different PPs and STs. The following should be noted: (441)

a) This annex identifies some of the more common statements likely to be used in an ST or PP. It does not in any sense provide an exhaustive checklist, and it is quite likely that you will need to identify additional statements for use in your PP or ST.

b) Although the examples can be copied and used verbatim, you should *always* consider whether the wording needs to be adapted or expanded for use in your PP or ST.

c) Not all statements listed here will be relevant to a given PP or ST.

Italicised text is used to help indicate where a generic term (e.g. a threat agent or the IT assets requiring protection) may be substituted by appropriate terminology specific to the PP or ST. (442)

Guidance on specifying cryptographic functionality (including their derivation from generic threats and security objectives) is provided in Annex C. (443)

B.1 Example Threats

T.ABUSE An undetected compromise of the *IT assets* may occur as a result of an *authorised user of the TOE* (intentionally or otherwise) performing actions the individual is authorised to perform.

T.ACCESS An *authorised user of the TOE* may access *information or resources* without having permission from the person who owns, or is responsible for, the *information or resource*.

T.ATTACK An undetected compromise of the *IT assets* may occur as a result of an attacker (whether an *insider or outsider*) attempting to perform actions that the individual is not authorised to perform.

T.CAPTURE An *attacker* may eavesdrop on, or otherwise capture, data being transferred across a network.

T.CONSUME An *authorised user of the TOE* consumes *global resources*, in a way which compromises the ability of other authorised users to access or use those resources.

T.COVERT An *authorised user of the TOE* may, intentionally or accidentally, transmit (via a covert channel) sensitive information to users who are not cleared to see it.

T.DENY A *user* may participate in the transfer of *information* (either as originator or recipient) and then subsequently deny having done so.

T.ENTRY Compromise of the *IT assets* may occur as a result of use of the TOE by an *authorised user* at an inappropriate time of day or in an inappropriate location.

T.EXPORT An *authorised user of the TOE* may export information from the TOE (in soft or hard copy form) which the recipient subsequently handles in a manner that is inconsistent with its sensitivity designation.

T.IMPERSON An *attacker (outsider or insider)* may gain unauthorised access to *information or resources* by impersonating an authorised user of the TOE.

T.INTEGRITY The integrity of *information* may be compromised due to user error, hardware errors, or transmission errors.

T.LINK An *attacker* may be able to observe multiple uses of *resources or services* by an entity and, by linking these uses, be able to deduce information which the entity wishes to be kept confidential.

T.MODIFY The integrity of *information* may be compromised due to the unauthorised modification or destruction of the *information* by an *attacker*.

T.OBSERVE An *attacker* could observe the legitimate use of a *resource or service* by a *user*, when the user wishes their use of that *resource or service* to be kept confidential.

T.SECRET An *authorised user of the TOE* may, intentionally or accidentally, observe *information stored in the TOE* that the user is not cleared to see.

The following threats will typically be addressed by security objectives for the environment rather than the TOE. (444)

TE.CRASH Human error or a failure of software, hardware or power supplies may cause an abrupt interruption to the operation of the TOE, resulting in the loss or corruption of *security-critical data.*

TE.BADMEDIA Aging of storage media, or improper storage or handling of removable media, may result in its corruption, leading to the loss or corruption of *security-critical data*.

TE.PHYSICAL Security-critical parts of the TOE may be subject to physical attack which may compromise security.

TE.PRIVILEGE Compromise of *IT assets* may occur as a result of actions taken by careless, wilfully negligent or hostile *administrators or other privileged users*.

TE.VIRUS Compromise of the integrity and/or availability of *IT assets* may occur as a result of an *authorised user of the TOE* unwittingly introducing a virus into the system.

B.2 Example Organisational Security Policies

Two typical examples are provided in this section. Specific organisations may of course have more detailed security policies than the ones presented below. (445)

P.DAC The right to access specific data objects is determined on the basis of:

a) the owner of the object; and

b) the identity of the subject attempting the access; and

c) the implicit and explicit access rights to the object granted to the subject by the object owner.

P.MAC The right to access information marked with a sensitivity designation is determined as follows:

a) an individual is only permitted to observe information if that individual is cleared to see it;

b) an individual may not downgrade the *sensitivity designation* of information, unless that individual has been given an explicit authorisation to perform such actions.

B.3 Example Assumptions

B.3.1 Physical assumptions

A.LOCATE The *processing resources of the TOE* are assumed to be located within controlled access facilities which will present unauthorised physical access.

A.PROTECT The TOE hardware and software critical to security policy enforcement is assumed to be physically protected from unauthorised modification by potentially hostile *outsiders*.

B.3.2 Personnel assumptions

A.ADMIN It is assumed that one or more *authorised administrators* are assigned who are competent to manage the TOE and the security of the information it contains, and who can be trusted not to deliberately abuse their privileges so as to undermine security.

A.ATTACK Attackers are assumed to have a *high* level of expertise, resources and motivation.

This assumption can be adapted as appropriate to the TOE security environment. Note that an assumption of this nature may be used in the definition of the threats, for example limiting the scope of a threat by excluding the possibility of attack from threat agents with particular levels of expertise, motivation or available resources. (446)

A.USER Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.

B.3.3 Connectivity Assumptions

A.DEVICE All connections to peripheral devices are assumed to reside within the controlled access facilities.

A.FIREWALL The firewall is assumed to be configured as the only network connection between the private network and the hostile network.

A.PEER Any other systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

B.4 Example Security Objectives for the TOE

O.ADMIN The TOE will provide facilities to enable an authorised administrator to effectively manage the TOE and its security functions, and will ensure that only authorised administrators are able to access such functionality.

O.ANON The TOE will provide the means of allowing a subject to use a *resource or service* without the user identity being disclosed to other *entities*.

O.AUDIT The TOE will provide the means of recording any security relevant events, so as to assist an administrator in the detection of potential attacks or misconfiguration of the TOE security features that would leave the TOE susceptible to attack, and also to hold users accountable for any actions they perform that are relevant to security.

O.DAC The TOE will provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the P.DAC security policy.

O.ENCRYPT The TOE will provide the means of protecting the confidentiality of *information* when it is transferred across a network between two end-systems.

O.ENTRY The TOE will have the capability of restricting user entry to it based on time and entry device location.

O.I&A The TOE will uniquely identify all users, and will authenticate the claimed identify before granting a user access to the TOE facilities.

O.INTEGRITY The TOE will provide the means of detecting loss of integrity affecting *information*.

O.LABEL The TOE will store and preserve the integrity of sensitivity labels for information it stores and processes. Data output (exported) by the TOE will have sensitivity labels that are an accurate representation of the corresponding internal sensitivity labels.

O.MAC The TOE will protect the confidentiality of information it is responsible for managing, in accordance with the P.MAC security policy, based directly on comparison of an individual's clearance or authorisation for the information, and the sensitivity designation of the information.

This security objective can, of course, be amended as appropriate for any particular information flow control policy objective. (447)

O.NOREPUD The TOE will provide a means of generating evidence which can be used to prevent an *originator* of *information* from successfully denying ever having sent that *information*, and evidence which can be used to prevent a *recipient* of *information* from successfully denying ever having received that *information*.

O.PROTECT The TOE will protect itself against external interference or tampering by untrusted subjects, or attempts by untrusted subjects to bypass the TOE security functions.

O.PSEUD The TOE will provide the means of allowing a subject to use a *resource or service* without the user identity being disclosed to other *entities*, whilst still being able to hold that entity accountable for that use.

O.RBAC The TOE will prevent users from gaining access to and performing operations on its resources for which their role is not explicitly authorised.

O.RESOURCE The TOE will provide the means of controlling the use of *resources* by its users and subjects so as to prevent unauthorised denial of service.

O.ROLLBACK The TOE will provide the means of returning to a well-defined valid state by permitting a user to undo transactions in the case of an incomplete series of transactions.

O.UNLINK The TOE will provide the means of allowing an *entity* to make multiple uses of resources or services without other *entities* being able to link those uses together.

O.UNOBS The TOE will provide the means of allowing a *user* to use a *resource or service* without other entities being able to observe that the *resource or service* is being used.

B.5 Example Security Objectives for the Environment

OE.AUDITLOG Administrators of the TOE must ensure that audit facilities are used and managed effectively. In particular:

a) Appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs before audit trail exhaustion to ensure sufficient free space.

b) Audit logs should be inspected on a regular basis, and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.

OE.AUTHDATA Those responsible for the TOE must ensure that the authentication data for each user account for the TOE is held securely and not disclosed to persons not authorised to use that account.

OE.CONNECT Those responsible for the TOE must ensure that no connections are provided to outside systems or users that would undermine IT security.

OE.INSTALL Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security.

OE.PHYSICAL Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.

OE.RECOVERY Those responsible for the TOE must ensure that procedures and/or mechanisms are in place to ensure that, after system failure or other discontinuity, recovery without compromise of IT security is obtained.

B.6 Example Mapping of Security Objectives to Threats

[Editor Note: the table below is proposed as an example of how one might construct a mapping from threats to security objectives for the TOE or its environment. The table cells indicate the form of the threat or security objective, and do not necessarily conform to the guidance provided elsewhere relating to the specification of threats and security objectives.] (448)

Asset	Threat	Security Objectives	
Data on storage media	Data is disclosed by illegally removing a medium.	Preventative	Control media removal. Prevent data disclosure (by encryption, etc.)
		Detective	Control media storage.
		Corrective	-
	Data is referenced, modified, deleted, or added from/to an application by an unauthorized person.	Preventative	Operation management (For example, restrict uses of an application program or an application terminal) Control the privilege to access data.
		Detective	Audit application operation log information, detect data tampering, and manage data sequence numbers.
		Corrective	Back up/Restore data.
	Data is disclosed by dumping a storage medium by an unauthorized person.	Preventative	Operation management (For example, restrict uses of a dump function or an operation terminal) Prevent data disclosure (by encryption, etc.)
		Detective	Audit operation log information.
	Remaining data on a medium is referenced.	Preventative	Clear the data area at the time of data deletion. Prevent data disclosure (by encryption, etc.)
	Data is copied illegally.	Preventative	Operation management (For example, restrict uses of a copy function or an application/ operation terminal) Control the privilege to access data. Prevent data disclosure (by encryption, etc.)
		Detective	Audit operation. Control the original (such as electronic watermark)
	Data is illegally used or its use is obstructed by changing the data access attribute by an unauthorized person.	Preventative	Operation management (For example, restrict uses of a data attribute modify function or an application/operation terminal) Control the privilege to access an attribute registration file.
		Detective	Audit operation.
		Corrective	Back up/Restore data.
	Data is got illegally by forging a file	Preventative	Operation management (For example, restrict uses of file create and delete functions or an operation terminal) Prevent data disclosure (by encryption, etc.)
		Detective	Audit file owners.

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
Data on storage media	Data is damaged by destruction of the medium.	Preventative	Physically manage the medium storage place and control access to the storage place. Adopt a dual configuration for storage media.
		Detective	Control media storage.
		Corrective	Back up/Restore data.
	Data is destroyed or its use is obstructed by a hardware failure of an medium I/O device	Preventative	Quality control of I/O devices Adopt a dual configuration for storage media.
		Detective	Detect failures (OS). Audit program execution log.
		Corrective	Back up/Restore data.
	Data is referenced, modified, deleted, or added by an unauthorized person using a command.	Preventative	Operation management (For example, restrict uses of operation commands or an operation terminal) Control the privilege to access data.
		Detective	Audit operation log information. detect data tampering, and manage data sequence numbers.
		Corrective	Back up/Restore data.
	Encrypted data cannot be decrypted due to loss of the secret key.	Preventative	Keep the secret key under strict management.
		Corrective	Recover the secret encryption key.
	Data is erroneously deleted by an authorized person.	Preventative	Provide high-quality operation manuals or automate operations. Prevent operating errors (for example, rechecking and sequentially registering the privilege to delete).
		Detective	Audit operation log information.
		Corrective	Back up/Restore data.
Data on telecommunication line	Data is tapped or destroyed on a telecommunication line	Preventative	Physically protect telecommunication lines or control equipment connections to lines. Prevent data disclosure, detect data tampering (by encryption transmitted data: VPN, SSL, IP sec, etc.)
		Detective	Detect data tampering.
		Corrective	Send data again.
	Data is tapped, tampered, deleted or added on a relay system.	Preventative	Operation management of a relay system (For example, restrict uses of LAN protocol analyser)

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
Data on tele-communication line	Data is illegally used by changing its destination, sender, or access attribute on a relay system.	Preventative	Protect control data to be transmitted (by encryption, etc.) Operation management of a relay system (Restrict uses of a debug function.)
		Detective	Detect control data tampering. Audit debug tool operation log information.
		Corrective	Send data again.
	Communications are disabled due to a line fault.	Preventative	Install dual telecommunication lines. Quality control of telecommunication lines
		Detective	Detect failures (OS).
		Corrective	Send data again.
	Communications are disabled due to a communication channel abnormality.	Preventative	Install dual channel devices. Quality control of communication channels
		Detective	Detect failures (OS).
		Corrective	Send data again.
	Data is illegally resent for illegal communications.	Preventative	Operation management of a relay system (For example, restrict program registration.)
		Detective	Prevent re-transmission (by assigning sequence numbers or time)
Application program	An application is executed by an unauthorized person.	Preventative	Control the privilege to execute a program. Operation management of a relay system (Restrict unnecessary program display.) Manage locations and route of execution. Provide safeguards during operator absence. Restrict uses of an application terminal.
		Detective	Audit program execution.
		Corrective	Related data backup/restore.
	Data in a program library is referenced, modified or deleted by an unauthorized person.	Preventative	Control the privilege to access a program library. Operation management (Restrict uses of a modify command.) Restrict uses of an operation terminal.
		Detective	Audit operation
		Corrective	Back up/Restore program.
	A program is illegally used or its use is obstructed by changing its access attribute by an unauthorized person.	Preventative	Control the privilege to execute a program. Control the privilege to access the program library directory. Operation management (Restrict uses of a modify command.)
		Detective	Audit operation.

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
Application program	An abnormality occurs during program execution due to a hardware failure of a computer.	Preventative	Adopt a dual hardware configuration. Quality control of hardware
		Detective	Detect failures (OS).
		Corrective	Hardware recovery
Application processing and data	Illegal application processing (such as Telnet and FTP) is executed.	Preventative	Control the privilege to execute a program. Firewall (application filtering) Clarify operation regulations.
		Detective	Audit program execution.
	Processing is obstructed (traffic attack such as requesting to process unnecessary data).	Preventative	Give priority to process processing. Prohibit a mail relay function.
		Detective	Audit network access.
	Data exchange or contents are denied.	Preventative	Take measures for preventing denial (such as storing an evidence using TTP or encryption function). Clarify operation rules.
	The original of data is denied.	Preventative	Reliable services (such as guarantee of an original) Clarify operation rules.
	Data is illegally sent.	Preventative	Control data flows (such as Firewall and rule DB control). Control the quality of application programs. Operation management (For example, restrict program registration.)
		Detective	Audit data access.
	Data or a program is illegally used using a remaining debug function.	Preventative	Control the privilege to access data and the privilege to execute a program. Operation management (Restrict uses of a debug function.)
		Detective	Audit application execution.
	A service function is inappropriately denied.	Preventative	Give priority to process processing. Control the quality of application programs. Provide education and regulations for application staff. Control the quality of processing hardware. Estimate the capacity of processing resources.
		Detective	Audit application execution.
	Contents are tampered or destroyed.	Preventative	Control the privilege to use contents. Control contents creation and downloading.
		Detective	Detect contents tampering.
		Corrective	Back up contents.

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
Application processing and data	Illegal operation	Preventative	Control the privilege to execute operations. Control the locations and routes of operations (remote, via Internet, etc.).
		Detective	Audit use of operations.
	Privacy is violated.	Preventative	Control the privilege to use privacy information. Use anonymity or a pen name (pseudonym). Guarantee unlinkability.
Display data	Data is seen by an unauthorized person.	Preventative	Isolate a display physically. Enforce operation rules.
	Illegal copy or printing	Preventative	Provide safeguards against an authorized person's absence. Restrict uses of copy and print functions. Enforce operation regulations.
		Detective	Control originals (electronic watermark)
Input data	Data is disclosed during input.	Preventative	Control access to an input terminal room. Enforce operation regulations.
	Input data is illegally taken out.	Preventative	Control the input data storage place. Enforce operation regulations.
		Corrective	Back up input data.
Printed data	Data is referenced or taken out by an unauthorized person.	Preventative	Physically control printed data. Enforce operation regulations.
	Illegal copy	Preventative	Provide safeguards against copying. Enforce operation regulations.
		Detective	Control originals (electronic watermark)
User data	A user (individual, system, terminal) cannot be identified.	Preventative	Identification at access Identification (ID assignment to each user/ system; IP address) Restrict locations (filtering).
		Detective	Audit identification processing.
	Disguise oneself using disclosed user (individual, system, terminal) identification information.	Preventative	User authentication Control identification information.
		Detective	Audit identification processing.
	A user is not identified.	Preventative	Prompt authentication Reliable identification. Authentication (encryption secrete key, password, belongings, physical characteristics) Call back
		Detective	Audit authentication processing.

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
User data	Disguise oneself using illegally disclosed authentication information.	Preventative	Adopt multiple authentication mechanisms. Server access management (Early detection by a victim; notification of authentication processing information) Save authentication information in a confidential medium. Protect authentication information (unidirectional encryption). Restrict access routes (such as public telecommunication lines and the Internet). One-time password
		Detective	Audit system access
		Corrective	Stop processing by the user.
	Disguise oneself by illegally inferring authentication information.	Preventative	Authentication (Preventing inference; limiting retry count) Server access management (Early detection by a victim; safeguards for not using a server for a long period) Adopt multiple authentication mechanisms. Control authentication information (such as preventing inference, long secrete encryption key, syntax rules, initial value change, and generation control)
		Detective	Audit system access
		Corrective	Stop processing by the user. Minimize influences (Effective period).
	Disguise oneself using invalid authentication information.	Preventative	Confirm validity of authentication information. Control authentication information (such as control nullified information).
		Detective	Audit system access
	An invalid privilege is used because of failure to register a modification of user privilege.	Preventative	Control users. (Immediately reflect a user privilege modification.)
		Detective	Audit system access
	A user's action is illegally disclosed (violation of privacy).	Preventative	Manage privilege to access user related log information. Use anonymity or a pen name (pseudonym). Guarantee unlinkability
		Detective	Audit system access
	Data transmission is denied.	Preventative	Prevent denial of transmission. Operation regulations.
		Detective	Audit data exchange.
	Data ownership is denied.	Preventative	Automatically register an owner at the time of data production.
		Detective	Audit system access.

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
User data	Data reception is denied.	Preventative	Prevent denial of reception. Operation regulations.
		Detective	Audit data exchange
	Data is sent to a wrong receiver due to disguise or a specification error.	Preventative	Destination authentication. Operation regulations.
		Detective	Audit data exchange
	Disguise oneself by forging authentication information.	Preventative	Manage privilege to access authentication information. Verify validity of authentication information. Control authentication information (such as preventing forging, reliable authentication organization, physically protecting belongings).
		Detective	Server access management (Early detection by a victim)
System Services and Data	A secret encryption key is decoded, undermining system security	Preventative	Produce a secret encryption key of sufficient strength and length and adopt a standard key delivery protocol.
		Detective	Audit system operations.
		Corrective	Set a new secret key.
	A system is illegally used by a disguised user during an operator's absence.	Preventative	Provide the necessary safeguards during an operator's absence (such as suspension, session disconnection, and re-authentication).
	System security is undermined by an authorized user's illegal act or mistake.	Preventative	Prevent an authorized user's mistakes (for example, by reconfirmation). Control user privileges (minimum privileges). Audit management, regulations, education, and penalties.
		Detective	Audit system operations
	Virus intrusion	Preventative	Virus check for program downloading and files with mail. Access control (Set an appropriate access privilege and protect files.) Prohibit loading data or program from the outside. Control software installation.
		Detective	Audit system operations
		Corrective	Take the necessary action (such as stopping the system and disconnecting an external system).

Table 3 - Example Mapping of Threats to Security Objectives

Asset	Threat	Security Objectives	
System Services and Data	Illegal intrusion to a system	Preventative	Check a user's identification, authentication, and privilege (at the time of accessing a barrier segment or log-in). System configuration management (such as connected equipment and external connections) User management.
		Detective	Audit system operations.
	Intrusion to a system by taking advantage of a known protocol defect (such as IP protocol and SendMail)	Preventative	Firewall (Filtering) Control access to system resources. Restrict access to the program or protocol.
		Detective	Audit system operations
	System security is undermined by illegal replacement of a system program.	Preventative	Control access to a system program library. Operation management (System program maintenance regulations)
		Detective	Audit program library access.
		Corrective	Back up programs.
	The service is stopped by system program destruction.	Preventative	Adopt a dual configuration for system program library. Medium management and operation management (system program library)
	Illegal system operation	Preventative	Control the privilege to execute operation commands. Operation management (Restrict uses of operation commands.)
		Detective	Audit operations.
Information equipment	Damaged or taken out.	Preventative	Dual configuration Control the access to the equipment location. Keep equipment (lines) under management during storage.
	Power is turned off.	Preventative	Backup power supply UPS
		Corrective	Recover power.

Table 3 - Example Mapping of Threats to Security Objectives

B.7 Example Security Functional Requirements

This section identifies, for example common or generic security functions, ISO/IEC 15408 Part 2 components which may be used to express appropriate SFRs. The reader is referred to ISO/IEC 15408 Part 2 Annexes for guidance relating to the use of specific ISO/IEC 15408 Part 2 functional components. See also Annex C for guidance on the specification of cryptographic functionality. (449)

These common or generic security functions are organised under the following headings: (450)

a) Identification and authentication;

b) Access control;

c) Audit;

d) Integrity;

e) Availability;

f) Privacy;

g) Data Exchange.

B.7.1 Identification and authentication requirements

Table 4 below covers common or generic identification and authentication requirements. (451)

Security Requirement		Functional Component
Logon controls	Identification of users	FIA_UID.1-2
	Authentication of users	FIA_UAU.1-2
	Limits on repeated login failures (e.g. enforcement of lockout or time delay)	FIA_AFL.1
	Trusted path for logon	FTP_TRP.1-2
	Time of day restriction of access to TOE	FTA_TSE.1
Password selection	Controls on selection of user-generated passwords (e.g. minimum length, password filters, password history)	FIA_SOS.1
	Automated generation of passwords by TOE	FIA_SOS.2
	Password lifetime (expiry) enforcement	FMT_SAE.1
Authentication data protection	Non-echoing of passwords during password entry	FIA_UAU.7
	Protection against unauthorised modification or observation	FMT_MTD.1
	Protection against replay attacks	FPT_RPL.1
	Protection against forgery or copying	FIA_UAU.3
	Protection against reuse (e.g. single use passwords)	FIA_UAU.4
	Trusted path for password change	FTP_TRP.1
Session suspension	Suspension following user inactivity	FTA_SSL.1
	Suspension at user request	FTA_SSL.2
	Termination following user inactivity	FTA_SSL.3

Table 4 - Functional Components for Identification and Authentication Requirements

Security Requirement		Functional Component
User accounts and profiles	Controls over creation, deletion, enabling or disabling of user accounts	FMT_MTD.1
	Definition of user security attributes contained in a user profile	FIA_ATD.1
	Controls over modification of user profiles (i.e. user security attributes)	FMT_MTD.1

Table 4 - Functional Components for Identification and Authentication Requirements

B.7.2 Access control requirements

Table 5 below covers common or generic access control requirements. (452)

Security Requirement		Functional Component
Discretionary Access Control	Scope of policy (subjects, objects and operations covered by the policy)	FDP_ACC.1-2
	Rules governing access by subjects to objects	FDP_ACF.1
	Privilege override of DAC policy	FDP_ACF.1
Controls on DAC attributes	Changing object permissions/ACLs	FMT_MSA.1
	Default protection on newly created objects	FMT_MSA.3
	Changing object owner	FMT_MSA.1
	Changing user group affiliations	FMT_MSA.1
Mandatory Access Control	Scope of policy (subjects, objects and operations covered by the policy)	FDP_IFC.1-2
	Rules governing access/information flow	FDP_IFF.2
	Privilege override of MAC policy	FDP_IFF.7-8
	Covert channel restrictions	FDP_IFF.3-6
Controls on MAC attributes	Changing object labels	FMT_MSA.1
	Default labels for newly created objects	FMT_MSA.3
	Changing user clearances	FMT_MSA.1
	Selection of session clearance at login	FTA_LSA.1
Export/import	Import of unlabelled data	FDP_ITC.1
	Export via communication channels/devices	FDP_ETC.1-2
	Labelling printed output	FDP_ETC.2

Table 5 - Functional Components for Access Control Requirements

Security Requirement		Functional Component
Information labels	Constraints on information label values	FDP_IFF.2.3
	Rules governing ‘floating’ labels	FDP_IFF.2.3
Object reuse	Protection of residual information in files, memory, etc.	FDP_RIP.1-2
Role based access control	Scope of policy (in terms of roles, operations)	FDP_ACC.1-2
	Rules controlling performance of operations	FDP_ACF.1[a]
	Identification of roles	FMT_SMR.1-2
	Two-man rule enforcement	FDP_ACF.1[b] FMT_SMR.2.3
Controls on RBAC attributes	Changing user privileges/authorisations	FMT_MSA.1
	Changing definitions of role capability	FMT_MSA.1
	Changing assignments of users to roles	FMT_MSA.1
Firewall access control	Subject-object information flow view (e.g. based on source/destination addresses and ports)	FDP_IFC.1-2 FDP_IFF.1
	Session-based view (e.g. application proxy)	FTA_TSE.1[c]

Table 5 - Functional Components for Access Control Requirements

[a] Other components exist (e.g. FMT_MOF.1, FMT_MSA.1, FMT_MTD.1) which can also serve to restrict the performance of specific operations to specifically identified roles.

[b] FDP_ACF.1 may be used to specify that particular operations require two distinct roles to authorise the action. FMT_SMR.2.3 can ensure that a user account cannot be assigned to both roles.

[c] See the worked example in Annex D. Alternatively FDP_IFC.1 and FDP_IFF.1 may be used.

B.7.3 Audit requirements

Table 6 below covers common or generic audit requirements. (453)

Security Requirement		Functional Component
Audit events	Specification of auditable events and information to be recorded	FAU_GEN.1
	Controls on selection of events to be audited	FMT_MTD.1
	Basis for selection of events to be audited	FAU_SEL.1
	Individual accountability of users	FAU_GEN.2

Table 6 - Functional Components for Audit Requirements

Security Requirement		Functional Component
Intrusion detection and response	Generation of alarms and response to imminent security violations	FAU_ARP.1
	Definition of rules, events, event sequences or patterns of system usage to be used to indicate potential or imminent security violations	FAU_SAA.1-4
Audit trail protection	Protection against loss of data e.g. due to audit trail saturation, interruptions to operation	FAU_STG.2-4
	Protection against unauthorised modification/ access	FAU_STG.1
Audit trail analysis/review	Provision of audit trail analysis/review tools	FAU_SAR.1-3

Table 6 - Functional Components for Audit Requirements

B.7.4 Integrity requirements

Table 7 below covers common or generic integrity requirements (including data authentication). (454)

Security Requirement		Functional Component
Data integrity	Detection of errors in stored data	FDP_SDI.2
	Generation and verification of checksums, one-way hash, message digest, etc.	FDP_DAU.1
	Rollback of transactions (e.g. database)	FDP_ROL.1-2
TOE integrity	Tamper detection	FPT_PHP.1-2
	Tamper resistance	FPT_PHP.3
Data authentication	Digital signature generation and verification	FDP_DAU.2
	Certificate generation and verification (e.g. public key certificates)	FDP_DAU.2

Table 7 - Functional Components for Integrity Requirements

B.7.5 Availability requirements

Table 8 below covers common or generic availability requirements. (455)

Security Requirement		Functional Component
Consumption of resources	Enforcement of limits/quotas on global resource consumption by users	FRU_RSA.1-2
	Limitation on number of logged in sessions by same user	FTA_MCS.1-2
Error handling	Maintenance of TOE operation in event of failures (fault tolerance)	FRU_FLT.1-2
	Error detection	FPT_TST.1
	Error recovery	FPT_RCV.1-4
Scheduling	Scheduling of activities/processes according to established priorities	FRU_PRS.1-2

Table 8 - Functional Components for Availability Requirements

B.7.6 Privacy requirements

Table 9 below covers common or generic privacy requirements. (456)

Security Requirement		Functional Component
User identity based privacy	Protection against disclosure of user identity when using services or resources	FPR_ANO.1-2
	Anonymous but accountable use of services or resources via a protected user alias	FPR_PSE.1-3
Resource/service based privacy	Protection against disclosure of linkage of multiple usage of resources or services to the same user	FPR_UNL.1
	Unobservable usage of specified resources or services	FPR_UNO.1-4

Table 9 - Functional Components for Privacy Requirements

B.7.7 Data exchange requirements

Table 10 below covers common or generic data exchange requirements. (457)

Security Requirement		Functional Component
Data exchange confidentiality	User data	FDP_UCT.1
	Security critical data, e.g. keys, passwords	FPT_ITC.1
Data exchange integrity	User data	FDP_UIT.1-3
	Security critical data, e.g. keys, passwords	FPT_ITI.1-2
Non-Repudiation	Proof of origin of exchanged information	FCO_NRO.1-2
	Proof of receipt of exchanged information	FCO_NRR.1-2

Table 10 - Functional Components for Data Exchange Requirements

Annex C Specifying Cryptographic Functionality

C.1 Introduction

C.1.1 Purpose and Scope

This annex contains guidance for Protection Profile (PP) and Security Target (ST) construction for cryptographic aspects of a Target of Evaluation (TOE) and not just for those TOEs which are cryptographic modules (which are, in effect, collections of cryptographic functions). However, the guidance is expressed in such a way that it can be combined to apply to TOEs which are cryptographic modules. Such guidance has been included to cover a wide range of such TOEs, and deal with the specific issues relating to specification of such functionality. (458)

The purpose of this annex is to provide guidance on how to specify cryptographic functionality and its supporting security requirements. It is **not** intended to provide guidance on cryptography or how to build a secure system using cryptographic functionality. (459)

Guidance on the application of individual functional components contained in the FCS (Cryptographic Support) class is provided in [15408-2] Annex E. Cryptographic functionality may be used to meet SFRs specified using other classes and families (e.g., Class FCO, and Families FDP_DAU, FDP_SDI, FDP_UCT, FDP_UIT, FIA_SOS, and FIA_UAU). In such cases the individual functional components specify the security requirements that cryptographic functionality must satisfy. The objectives in class FCS should be used when the cryptographic functionality of the TOE is sought by consumers. (460)

Whilst specific assurance requirements are discussed in this document, the scope of the guidance excludes discussion of the strength of cryptography, as well as actual assurance levels. The assurance requirements for the TOE should be determined based on the sensitivity of the application and the anticipated threats and vulnerabilities that can be effectively countered by the assurance requirements. This is discussed in detail in Chapter 5 of this guide. (461)

C.1.2 Terminology

The terminology used in this annex is based on that defined in [15408-1] clause 2 and in Part 8 of ISO/IEC DIS 2382 [ISO-2382]. In addition, the following terms are defined to facilitate the understanding of the concepts presented in this document: (462)

Access Mode — A type of operation specified by an access right. Example: read, write, execute, append, modify, delete, create, etc. Also see Access Type in [ISO-2382]. (463)

Black Data — Data of which information content is not readily accessible because it is protected by **encryption**. Examples of data are messages, files, **cryptographic key**s, etc. (464)

Cryptographic Algorithm — A set of mathematical rules to transform data input into an output based on other input parameters such as **cryptographic keys** and **initialisation vector**s. (465)

Cryptographic Checksum — A relatively short value derived from data by use of a **cryptographic algorithm**. It is a function of data, a **secret key**, and, possibly, an **initialisation**

vector and is generally attached to the data in order to perform data integrity authentication. Also see Message Authentication Code in [ISO-2382]. (466)

Cryptographic Checksum Generation — The process of generating the **cryptographic checksum** for the purpose of attaching it to the data. (467)

Cryptographic Checksum Verification — The process of generating the **cryptographic checksum** for the purpose of verifying the attached **cryptographic checksum**. (468)

Cryptographic Function — One of the computations performed with a **cryptographic algorithm**. Examples: **encryption**, **decryption**, **digital signature generation**, **digital signature verification,** etc. (469)

Cryptographic Functionality — One or more of the **cryptographic function**s embedded in a TOE. (470)

Cryptographic Key — A value that controls the running of a **cryptographic algorithm** and its outcome. Also, see Key in [ISO-2382]. (471)

Cryptographic Key Access — An operation performed on a **cryptographic key.** Examples of operation/access are: read, write, archive, backup, recovery. (472)

Cryptographic Key Agreement — A **cryptographic function** that allows two parties to compute a shared **secret key**. (473)

Cryptographic Key Archive — An operation to store the **cryptographic key** in a permanent or long-term storage medium. (474)

Cryptographic Key Backup — An operation to backup the **cryptographic key** so that it can be reused in case the original **cryptographic key** is deleted, modified, destroyed, or becomes inaccessible. (475)

Cryptographic Key Destruction — A process to delete (zeroise) a **cryptographic key**. (476)

Cryptographic Key Distribution — A process to provide **cryptographic key**s to users, processes, TOE units, etc. (477)

Cryptographic Key Escrow — A process of providing a **cryptographic key** to a trusted third party who is obliged to release that key to authorised parties. (478)

Cryptographic Key Generation — A function to create a **cryptographic key**. (479)

Cryptographic Key Management — A process to manage the life-cycle of **cryptographic key**s from generation through distribution to archival and destruction. (480)

Cryptographic Key Recovery — A process to restore a **cryptographic key** from any of the sources including archive, backup, and escrow. (481)

Cryptographic Mechanism — A process or technique that involves one or more **cryptographic function**s. (482)

Cryptographic Operation — See **Cryptographic Function.** (483)

Cryptographic Variable (CV) — A value or series of values required for the operation of the **cryptographic algorithm** in order to transform the algorithm input to output. Examples of cryptographic variable are **cryptographic key**s (secret, public, private, etc.), **public key parameters**, and **initialisation vectors**. (Note that plaintext, cyphertext and hash values are not considered to be cryptographic variables.) (484)

Data Path — Logical or physical route over which data passes (or flows through) (485)

Digital Signature — See Digital Signature in [ISO-2382]. (486)

Digital Signature Generation — The process of generating a **digital signature**. (487)

Digital Signature Verification — The process of verifying a generated **digital signature**. (488)

Hashing or **Hash Value** — See **Secure Hash**. (489)

Initialisation Vector — A vector (series of bits) used in conjunction with a **cryptographic key** to define the starting point of **encryption** within a **cryptographic algorithm**. (490)

Invocation Parameter — A secret (e.g., a password or personal identification number) which is supplied to a TOE to access a **cryptographic function**. (491)

Message Digest — See **Secure Hash.** (492)

Non-Repudiation — The inability of an entity to deny having participated in a (certain part of a) communication. (493)

Other Critical Security Parameter — See **Invocation Parameter**. (494)

Private Key — One of the keys of a **public key pair**. Its confidentiality must be protected because it will be used for **decryption**, **digital signature generation** or **cryptographic key agreement**. (495)

Public Key — One of the keys of a **public key pair** that can be made public. Some public keys are used for **encryption**, some for **digital signature verification**, and some for **cryptographic key agreement**. (496)

Public Key Pair — A pair of mathematically related keys where deriving the **private key** from the associated **public key** should be computationally infeasible. (497)

Red Data — of which the information content is readily accessible because it is not protected by **encryption**. Examples of data are messages, files, **cryptographic keys**, etc. (498)

Red/Black Separation — Keeping the data paths for **red data** and **black data** logically or physically separate. For example, **red data** and **black data** should never travel over common physical wires and never occupy the same area of memory. (499)

Secret Key — A key used with a **cryptographic algorithm** for both **encryption** and **decryption**. (500)

Secure Hash — A value that is a result of applying an algorithm to a message such that it is computationally infeasible to derive the message from the result (secure hash), derive another message that gives the same hash given the message and the secure hash, and find two messages that produce the same hash. Usually, the secure hash is considerably shorter that the message or file from which it is derived. Also known as **hash value**, **message digest**. (501)

Tamper Detection Envelope — An area surrounding the TOE for which tamper (breach or attempt to intrude) can be detected. (502)

Zeroisation — A method of electronically erasing stored data by altering the data so that the originally stored data can not be recovered. (503)

Zeroisation Circuit — An electronic circuit to achieve **zeroisation.** (504)

Zeroisation Circuitry — See **Zeroisation Circuit.** (505)

C.2 Overview of cryptography

C.2.1 What is cryptography?

Cryptography is the science or art which embodies principles, means and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorised use. Its science component is founded on mathematics while the art arises out of many years of practical experience. It includes (but is not limited to): (506)

a) digital signature generation and/or verification;

b) cryptographic checksum generation for integrity and/or for verification of checksum;

c) secure hash (message or file digest) computation;

d) data encryption and/or decryption;

e) cryptographic key encryption and/or decryption;

f) cryptographic key agreement.

Cryptographic functionality can be used to meet several high-level security objectives. These include (but are not limited to): (507)

a) confidentiality;

b) integrity;

c) identification and authentication;

d) non-repudiation;

e) trusted path;

f) trusted channel;

g) data separation.

Cryptographic functionality should utilise suitable cryptographic algorithms and cryptographic key sizes, as well as secure cryptographic protocols and sound cryptographic engineering. (508)

C.2.2 Why use cryptography?

PP and ST developers should note that cryptographic functionality may only be one of several forms of functionality that might be used to meet a security objective. The selection of cryptographic functionality to meet a security objective should therefore be considered in the context of defining an overall well balanced set of procedural, physical and IT security measures. (509)

There may be a number of reasons to choose cryptography over other forms of security functionality: (510)

a) Only cryptographic functions may meet the desired security objective(s).

Example: *transmission of information over unprotected wire or over the air (i.e., across the public domain). Cryptography is the only functionality that provides confidentiality or integrity to data communicated under these circumstances.*

b) Cryptographic functions may provide the appropriate level of security to counter the anticipated threats.

Example: *authentication over an insecure network. Cryptography can be used to protect against eavesdropping or replay of authentication information. The authentication means is sometimes implemented by a “challenge-response” mechanism.*

c) Cryptographic functions may be the simplest/easiest/cheapest to implement, operate and/or use.

d) Cryptographic functions may be used as part of a number of different means to protect information (this is also known as the “strength-in-depth” concept).

Example: *The data is protected against unauthorised disclosure using the ‘traditional’ computer security access controls and/or physical security means. In order to provide an additional level of protection against failure of these mechanisms, the data is also encrypted. Thus, if an adversary were to be able to defeat the access controls, (s)he will also have to defeat the cryptographic mechanism in order to obtain the data.*

C.2.3 Why use cryptographic standards?

In a wider context, cryptographic functions may need to conform to a specified standard (which may be either international, national, industrial or organisational in nature) for one or more of the following reasons: (511)

a) It may help establish a common acceptable level of security;

b) It may facilitate interoperability;

c) It may facilitate mutual recognition;

d) It may be required by the organisational security policy;

e) It may facilitate the inclusion of desired functionality.

C.3 Deriving the security requirements

This section identifies cryptography-related aspects to consider when specifying threats, organisational security policies and security objectives for TOEs containing cryptographic functionality, and where cryptography needs to be considered when deriving the security requirements and assumptions that should be specified in a PP or ST. Guidance in this section is only indicative of the issues to consider when deriving the security requirement for a TOE containing cryptographic functionality, and may not take into account parallel, non-cryptographic issues. (512)

C.3.1 Threats

Typically known or assumed threats to IT assets in a TOE containing cryptographic functionality should be specified in the PP or ST. These threats may, or may not, be countered by the TOE.(513)

As stated in Chapter 3 to this guide, a clear specification of a threat should detail the source of the threat (or threat agent), the IT assets under attack and the form of attack. Furthermore, only events which *directly* compromise the IT assets, rather than attacks based on flaws or weaknesses in the TOE implementation should usually be included. (514)

This means that one approach that can be taken would be to define the threats as a ‘3-tuple’ comprising the source of the threat/threat agent, the IT asset under attack by the threat agent, and form of threat. The threats can then be used to define security objectives, which in turn can be refined into IT security requirements. (515)

C.3.1.1 Typical sources of threats

Typical sources of threats (or threat agents) to a TOE containing cryptographic functionality include (but are not limited to): (516)

a) authorised users of the TOE;

b) unauthorised individuals;

Note that in this context, an authorised user is one who is authorised to access defined IT asset(s). (517)

C.3.1.2 Typical cryptography-related IT assets

Typical types of cryptography-related IT assets in a TOE requiring protection include (but are not limited to): (518)

a) cryptographic variables (including secret keys, private keys, public keys, public key parameters, initialisation vectors, etc.);

b) input to and output from the cryptographic function (e.g., plaintext and ciphertext);

c) the implementation of the cryptographic algorithm in hardware, software and/or firmware;

d) invocation parameters (also known as ‘other critical security parameters’).

C.3.1.3 Typical forms of attack

Cryptography-related IT assets typically need to be protected from several forms of attack. These include (but are not limited to): (519)

a) detection of electromagnetic radiation emanations from the TOE;

b) impersonation of authorised users of the TOE;

c) induction of errors in the TOE;

d) incorrect use (i.e., operation or administration) of the TOE;

e) malfunction of the hardware, firmware or software comprising the TOE;

f) physical attack.

(Note that these attacks are not necessarily restricted to cryptographic assets.) (520)

C.3.1.4 Typical threats

Using the sample inputs to the threat ‘3-tuple’ identified in the preceding sub-sections, there are up to 48 specific threats (i.e., 2 threat agents × 6 forms of attack × 4 cryptography-related IT assets). Table 11 below provides examples of threats derived in this manner. (521)

T.Type	Threat
T.EMI	Cryptography-related IT assets may be disclosed to an unauthorised individual or user via the electromagnetic emanations from the TOE.
T.IMPERSON	An attacker (outsider or insider) may impersonate an authorised user of the TOE.
T.ERROR	An unauthorised individual or user of the TOE may cause unauthorised disclosure or modification of cryptography-related IT assets by inducing errors in the TOE.
T.MODIFY	The integrity of information may be compromised due to the unauthorised modification or destruction of the information by an attacker.
T.ATTACK	An undetected compromise of the cryptography-related IT assets may occur as a result of an attacker (whether an insider or outsider) attempting to perform actions that the individual is not authorised to perform.
T.ABUSE	An undetected compromise of the cryptography-related IT assets may occur as a result of an authorised user of the TOE (intentionally or otherwise) performing actions the individual is authorised to perform.

Table 11 - Typical Threats Relevant to Cryptographic Assets

T.Type	Threat
T.MAL	Cryptography-related IT assets may be modified or disclosed to an unauthorised individual or user of the TOE, through malfunction of the TOE.
T.PHYSICAL	Security-critical parts of the TOE may be subject to physical attack which may compromise security.

Table 11 - Typical Threats Relevant to Cryptographic Assets

C.3.2 Organisational security policies

The OSPs (if any) with which a TOE may need to comply should also be specified in the PP or ST. OSP statements of relevance to the cryptographic functionality in a TOE and which cannot be sensibly included within or implied by a threat description should be documented. These include (but are not limited to) statements for: (522)

a) identification and authentication policy;

b) user access control policy;

c) audit and accountability policy;

d) cryptographic key management policy;

e) physical security policy;

f) emanations policy.

PP/ST developers may also wish to apply these OSP statements to non-cryptography-related aspects of the TOE. (523)

Further information on the various parts of the security policy for a TOE containing cryptographic functionality and how they can be represented in ISO/IEC 15408 is addressed in Section C.4.5. (524)

C.3.3 Security objectives

Typical security objectives are shown in Table 12 below. (525)

O.Type	Security Objective
O.I&A	The TOE must uniquely identify all users, and must authenticate the claimed identify before granting a user access to the TOE facilities.
O.DAC	The TOE must provide its users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of individual users or identified groups of users, and in accordance with the set of rules defined by the discretionary security policy.

Table 12 - Example Security Objectives for the TOE

O.Type	Security Objective
O.PHP	The TOE should protect itself and cryptography-related IT assets therein from unauthorised physical access, modification or use.
O.INTEGRITY	The TOE must provide the means of detecting loss of integrity affecting information.
O.FAILSAFE	In the event of an error occurring, the TOE should preserve a secure state.
O.ADMIN	The TOE must provide functionality which enables an authorised administrator to effectively manage the TOE and its security functions, and must ensure that only authorised administrators are able to access such functionality.
O.EMI	Procedural and physical measures should be taken to prevent the disclosure of cryptography-related IT assets to unauthorised individuals or users via the electromagnetic emanations of the TOE.
O.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.

Table 12 - Example Security Objectives for the TOE

Note that O.EMI and O.PHYSICAL are security objectives for the environment. The rest are the security objectives for the TOE. Other security objectives for the environment may address: (526)

a) procedures for the handling and storage of cryptography-related IT assets input into and output by a TOE;

b) the procedures for the operation and maintenance of a TOE;

c) the level of trust to be placed in authorised users of the TOE;

d) the training of the authorised users (e.g. cryptographic key custodians, maintenance personnel, general users) who will interact in some way with the TOE;

e) the physical measures needed to protect the TOE;

f) environmental operating constraints (including electromagnetic emanation limitations) on the TOE;

g) the IT security environment outside the TOE (e.g. limitations on the type of software present outside the TOE, use of an underlying trusted operating system to enforce the TOE access control policy).

C.3.3.1 Security objectives rationale

An indicative demonstration of the suitability of the security objectives to counter the threats is shown in the Table 13 below. This table does not necessarily present the level of detail needed for the security objective suitability aspect of a PP or ST rationale. (527)

T.Type	Related O.Type and Rationale
T.EMI	O.EMI - Requiring the use of procedural and physical measures (e.g. room shielding, distance from the public domain) should reduce the risk of disclosure of cryptography-related IT assets through the emanations from the TOE.
T.IMPERSON	O.I&A - Requiring reliable identification and authentication of a user should reduce the risk of user impersonation.
T.ERROR	O.FAILSAFE - Requiring the TOE to preserve a secure state in the event of an error occurring should reduce the exposure due to inadvertent modification or disclosure of cryptography-related IT assets.
T.ABUSE	O.DAC - Requiring all accesses to the TOE to conform to a specified access control policy should reduce the risk of users performing any operations to which they do not require access.
T.MAL	O.INTEGRITY - Requiring TOE to detect loss of integrity increases the chances of error detection. O.FAILSAFE - Requiring the TOE to preserve a secure state in the event of an error occurring should reduce the exposure due to inadvertent modification or disclosure of cryptography-related IT assets.
T.PHYSICAL	O.PHP – Requiring protection against physical attacks should reduce the risk of physical attacks. O.PHYSICAL - Requiring the use of procedural and physical measures to limit physical access to the TOE to only those users required and authorised to have physical access should reduce the risk of a physical attack on the TOE being performed.
T.MODIFY	O.INTEGRITY – The ability to detect loss of integrity should reduce the chances of attacker modifying the cryptography-related IT assets. O.ADMIN – Proper configuration and administration of the TOE should reduce the risk of modification.
T.ATTACK	O.I&A - Requiring reliable identification and authentication of a user should reduce the risk of unauthorised access. O.DAC - Requiring all accesses to the TOE to conform to a specified access control policy should reduce the risk of users performing any operations to which they do not require access.

Table 13 - Security Objectives Rationale

C.3.4 Security requirements

Security objectives may be refined into IT security requirements as indicated in Table 14 below. (528)

O.Type	Security Objective	ISO/IEC 15408 Component
O.I&A	The TOE must uniquely identify all users, and must authenticate the claimed identify before granting a user access to the TOE and the cryptography-related IT assets therein.	FIA_UID.1-2 FIA_UAU.1-5
O.DAC	The TOE must provide its users with the means of controlling and limiting access to the cryptography-related IT assets in accordance with a specified access control policy.	FDP_ACC.1-2 FDP_ACF.1
O.PHP	The TOE should protect itself and cryptography-related IT assets therein from unauthorised physical access, modification or use.	FPT_PHP.1-3
O.INTEGRITY	The TOE must provide the means of detecting loss of integrity affecting information.	FPT_AMT.1 FPT_TST.1.
O.FAILSAFE	In the event of an error occurring, the TOE should preserve a secure state.	FPT_FLS.1-4
O.ADMIN	The TOE must provide functionality which enables an authorised administrator to administer cryptographic keys in accordance with a specified cryptographic key management policy.	FCS_CKM.1-4 FCS_COP.1
O.EMI	Procedural and physical measures should be taken to prevent the disclosure of cryptography-related IT assets to unauthorised individuals or users via the electromagnetic emanations of the TOE.	AGD_ADM.1 AGD_USR.1 Security operating procedures
O.PHYSICAL	Those responsible for the TOE must ensure that those parts of the TOE that are critical to security policy enforcement are protected from physical attack which might compromise IT security.	Security operating procedures

Table 14 - Derivation of Security Requirements from Security Objectives

C.4 Expressing IT security requirements

C.4.1 Introduction

This section explains exactly how the IT security requirements that may need to be included in a TOE containing cryptographic functionality can be expressed in a PP or ST using ISO/IEC 15408. (529)

Detailed discussion of the contents of the TOE security environment (threats, OSPs and assumptions) and security objectives parts of a PP or ST are made in section C.3. (530)

Developers should remember that this guidance only applies to the production of PPs and STs for those TOEs which contain cryptographic functionality. It is only *indicative* of the components and families that might be of use in specifying the requirements for such a TOE and may not take into account functionality needed for parallel, non-cryptographic issues. It does not take into account the need for augmented requirements or the requirements of any predefined functional or assurance packages (such as a claimed evaluation assurance level). Neither does it explicitly take into account all additional component interdependencies. (531)

C.4.2 Traditional concerns in cryptographic design and implementation

Cryptographic equipment designers and implementers are traditionally concerned with certain vulnerabilities which have been determined from operational and engineering experience, principally with respect to cryptographic hardware. Table 15 summarises these traditional vulnerabilities and their traditional solutions. (532)

Vulnerability	Traditional solution
Mixing of data and keys	Separate physical ports
Exploitation of maintenance access port	Specific maintenance role
Mixing of plaintext and ciphertext	Separate input and output paths Red/black data separation
Release of sensitive information due to cryptographic malfunction	Two internal, independent actions to release sensitive information Disconnect output data path from key generation, key entry, and key zeroisation circuitry
Unauthorised access	Identification and authentication Access control on functions, services, and data
Design errors	Finite state machine design
Physical attack	Physical security measures
Spurious hardware errors	Self-testing
Electromagnetic emanations	Electromagnetic emanations control standards

Table 15 - Traditional Vulnerabilities and Solutions

The following table summarises how the solutions to these traditional vulnerabilities are represented using ISO/IEC 15408. (533)

Vulnerability	ISO/IEC 15408 representation
Mixing of data and keys	Modularity (ADV_INT)
Exploitation of maintenance access port	Maintenance access control SFP (FDP_ACC, FDP_ACF)
Mixing of plaintext and ciphertext	Modularity and information hiding (ADV_INT)
Release of sensitive information due to cryptographic malfunction	Fail secure (FPT_FLS) Modularity and information hiding (ADV_INT)
Unauthorised access	Identification and authentication (FIA_UID, FIA_UAU, FIA_ATD) User access control SFP (FDP_ACC, FDP_ACF)
Design errors	Semiformal and formal design (ADV_HLD, ADV_LLD)
Physical attack	Physical security (FPT_PHP)
Spurious hardware errors	Fail secure (FPT_FLS) Self-testing (FPT_AMT, FPT_TST)
Electromagnetic emanations	Emanations policy Assumptions

Table 16 - ISO/IEC 15408 Representations of Traditional Solutions

For ease of explanation of these ISO/IEC 15408 representations, as well as the typical ISO/IEC 15408 representations identified in Table 14, the expression of the typical security requirements of a TOE containing cryptographic functionality is considered under the following six headings:(534)

a) TOE definition;

b) TOE design and implementation;

c) TOE security policy;

d) TOE security functionality;

e) TOE testing;

f) TOE operation.

C.4.3 TOE definition

C.4.3.1 Guidance

The TOE, its components, functions and interfaces should all be fully defined in the PP/ST, i.e. there should be a functional specification for the TOE. This is to ensure that all the functional requirements defined in the PP/ST are addressed and that the TSP is enforced by the TSF. This also means that a TOE security policy which is consistent with the functional specification also has to be defined (see also Section C.4.5). (535)

Note that TOE definition is distinct from TOE design in that the definition deals with defining the TOE functionality and the physical/logical boundaries of the TOE. The TOE design deals with providing a refinement of the functional specification that can be implemented. (536)

C.4.3.2 ISO/IEC 15408 Representation

Component(s) from the ADV_FSP (Functional Specification) family should be used to express the requirement for a high level description of the user-visible interface and behaviour of the TSF. (537)

If there is a requirement for a semiformal design (e.g. a finite state machine design), then the ADV_FSP.3 (Semiformal functional specification) component should be used. If there is a requirement for security policy model, then the ADV_SPM (Security Policy Modelling) family should be used. (538)

C.4.4 TOE design and implementation

C.4.4.1 General assurance

Guidance

Due care should be taken to minimise and, wherever possible, eliminate design and implementation errors. It should be demonstrated in the PP/ST that the TOE at least provides a high-level architecture appropriate to implement the claimed functional requirements. (539)

If greater confidence in the design and its implementation are required then it may be necessary to demonstrate that the lower levels of design (potentially down to the lowest level) also express the required functionality and have been correctly refined from the higher-levels of design. (540)

ISO/IEC 15408 Representation

Appropriate components from the following families should be selected to meet the desired confidence in the correctness of the TOE design and implementation. (541)

a) ADV_HLD (High-level design)

b) ADV_LLD (Low-level design)

c) ADV_RCR (Representation correspondence)

d) ALC_TAT (Tools and techniques).

Component(s) from the ADV_HLD family should be used for expressing the requirement to describe the TSF in terms of major structural units (i.e. sub-systems) and relating these units to the functions that they contain. The ADV_HLD.2 (Security enforcing high-level design) component should be used if there is a requirement to distinguish the cryptographic boundary of the TOE from the overall TOE boundary. (542)

Component(s) from the ADV_LLD family should be used for expressing the requirement to describe the internal workings of the TSF in terms of modules and their interrelationships and dependencies. (543)

Component(s) from the ADV_RCR family should be used when there is a requirement to demonstrate the correspondence between various representations of the design. (544)

The ALC_TAT.2 component should be used when there is a requirement for the development to be performed in accordance with a defined implementation standard (e.g. coding standard). (545)

C.4.4.2 Modular design

Guidance

As previously stated, cryptographic designers and implementers are typically concerned that an error in one part of the TOE may influence other parts of the TOE, and that information from one part of the TOE may be available to the other parts of the TOE that do not require that information. These concerns have led to the following types of traditional requirements: (546)

a) All input data entering the TOE via the data input interface shall pass only through the input data path;

b) All output data exiting the TOE via the data output interface shall pass only through the output data path;

c) The data output path shall be logically disconnected from the circuitry and processes performing key generation, manual key entry or key zeroisation;

d) The TOE shall keep separate data paths for red data and black data.

The intent of these specific requirements is to provide engineering guidance that lead to modular design, reduce complexity, and minimise effects of errors in one part of the system. (547)

ISO/IEC 15408 Representation

In order to express requirements for modular design of the TOE in a PP/ST, component(s) from the following families should be selected: (548)

a) ADV_FSP (Functional specification)

b) ADV_HLD (High-level design)

c) ADV_INT (TSF internals)

d) ADV_LLD (Low-level design).

For example, the low level design shows all the data flows and can be used to ensure that the inputs, outputs, plaintext, and cyphertext are accessed only by the components of the TOE that need them. The modularity and layering requirements help ensure that the TOE is designed using sound engineering principles and hence data is accessed only by the component of the TOE that need it. (549)

Of direct relevance to this are the following elements from the ADV_INT.3 (Minimisation of complexity) component from the ADV_INT (TSF Internals) family: (550)

ADV_INT.3.3CThe architectural description shall describe how the TSF design provides for largely independent modules that avoid unnecessary interactions.

ADV_INT.3.5CThe architectural description shall show that mutual interactions have been minimised, and justify those that remain.

ADV_INT.3.6CThe architectural description shall describe how the entire TSF has been structured to minimise complexity.

C.4.5 TOE security policy

C.4.5.1 Introduction

The PP/ST should describe the TOE security policy. The security policy for a TOE containing cryptographic functionality should include, but may not be limited to, the following aspects: (551)

a) identification and authentication policy;

b) user access control policy;

c) audit and accounting policy;

d) cryptographic key management policy;

e) physical security policy;

f) electromagnetic emanations policy.

Expression of these security policies are typically achieved through a combination of statements of organisational security policy (e.g., reference to electromagnetic emanations standards, specification of the user access control policy), assumptions (e.g., physical and procedural measures needed to protect the TOE) and by TOE IT functional requirements (e.g., specifying the functional mechanisms which implement the user access control policy). (552)

C.4.5.2 Identification and authentication policy

Guidance

The types of users and/or roles and the means used to authenticate them should be specified in the PP/ST. Typical cryptography-related roles include: (553)

a) cryptographic officer/custodian;

b) system maintainer;

c) system auditor;

d) system security officer;

e) user/operator.

ISO/IEC 15408 Representation

Appropriate components from the FIA class should be selected to express requirements to establish and verify a claimed user identity. Typically, component(s) from the following families should be selected: (554)

a) FIA_UID (User Identification)

b) FIA_UAU (User Authentication)

c) FIA_ATD (User Attribute Definition).

Component(s) from the FIA_UID family should be used to define the conditions under which users shall be required to identify themselves before performing any other actions that are to be mediated by the TSF and which require user identification. (555)

Component(s) from the FIA_UAU family should be used to define the user authentication mechanisms supported by the TSF. (556)

Component(s) from the FIA_ATD family should be used to define the security attributes for a user. Component(s) from the FIA_ATD family should be used to define the cryptographic key information as a user attribute. (557)

Protection of authentication information against capture and replay may be further achieved using components from the FTP_TRP (Trusted Path) family and/or FIA_UAU (FIA_UAU.3 – Unforgeable authentication; and FIA_UAU.4 – Single-use authentication mechanisms). Section C.4.6.3 contains further discussion of the use of trusted path. (558)

C.4.5.3 User access control policy

Guidance

The TOE should enforce user access to cryptographic IT assets in accordance with a specified user access control policy. In the context of a TOE containing cryptographic functionality, the elements of a user access control policy are: (559)

a) the user roles;

b) the services that can be accessed;

c) the critical security parameters, e.g. cryptographic keys (both unencrypted and encrypted), other critical security parameters (such as authentication data);

d) the modes of access (e.g., read, write, execute, delete, etc.) to the services and critical security parameters.

User access to the TOE may be based on a role-based access control (RBAC) policy, an identity-based access control (IBAC) policy or a combination of the two. (560)

In some designs, maintenance personnel may be able to bypass the access control mechanisms of a TOE containing cryptographic functionality. Thus, an enforceable maintenance access policy may also need to be defined. This policy must address how, if at all, user information shall be protected from access by the maintenance personnel. (This may be achieved by procedural and/or technical means.) (561)

Example: (562)

Prior to maintenance personnel being allowed access to the TOE:

a) *All the plaintext information shall be encrypted using a master key.*

b) *The master key shall be output and the copy internal to the TOE shall then be zeroised.*

After the maintenance personnel have performed their maintenance task(s), the master key shall be loaded in the TOE to decrypt the previously encrypted information.

ISO/IEC 15408 Representation

Component(s) from the following families should be selected: (563)

a) FDP_ACC (Access Control Policy)

b) FDP_ACF (Access Control Functions)

c) FDP_IFC (Information Flow Control Policy)

Cryptographic keys should be stored in and protected by the TOE. User keys may be protected in accordance with an access control policy using a component from the FDP_ACC family. System keys may be protected in accordance with the FMT_MTD family. (564)

At a minimum, the FDP_ACC.1 component should be used. The Security Function Policy (SFP) should be defined using this component to control access to cryptography-related IT assets for all subjects. Depending on the other functions and SFP for the whole TOE, the FDP_ACC.2 component may be more appropriate. (565)

FDP_ACF.1 should be used to define the requirement to enforce the user access control SFP as follows: (566)

FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the user access control policy to objects based on [assignment: *list of object attributes*]

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: subject is allowed to perform the desired cryptographic operation using [assignment: *the object*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

The subjects in the above case are the users or active abstract entities (e.g., a process) acting on behalf of the user. (567)

Each subject has the attribute of user identity, current role(s), and current time (if appropriate). (568)

The objects in the above case are the plaintext data and unencrypted cryptographic keys. The objects may also include the following additional items: cyphertext data and encrypted cryptographic keys. (569)

Examples of object attributes include the object's cryptographic function, role associated with the object, users associated with the object, object identifier, and the validity period (if appropriate) for the object. (570)

This security policy does not address the protection of plaintext or protected (e.g., encrypted) critical security parameters, such as the authentication information. To protect authentication information (even if encryption is used), appropriate families and components from the FMT class should be used (for example, FMT_MSA family should be used to specify a policy governing the protection of authentication data). (571)

If the subject attributes, the desired cryptographic function, and the object attributes satisfy the rule(s) specified with FDP_ACF.1, then the function is allowed to be performed. (572)

The cryptographic key information should also be protected in accordance with the information flow control policy. The information flow control policy should be defined by using a component of the FDP_IFC family. (573)

C.4.5.4 Audit and accountability policy

Guidance

The auditing and accountability requirements for the TOE (if any) should be defined in the PP/ST. (574)

Procedural requirements may include: (575)

a) when to inspect the TOE for physical tampering or errors (examples include within a specified minimum period, whenever a user suspects tampering or that an unexpected error has occurred, whenever a user may have violated the environmental assumptions, whenever a user may have violated the responsibilities for the physical protection of the TOE).

b) how to detect and report physical tampering or errors.

If the TOE does implement auditing and accountability functionality, then developers should remember to ensure that sensitive information (e.g., secret or private cryptographic keys) is not included in any form of audit record. (576)

ISO/IEC 15408 Representation

Assumptions should be used to express procedural accounting and audit requirements in the PP/ST. (577)

Minimal and basic levels of audit are defined for both the FCS_CKM and FCS_COP families. Further information on the use of audit components, as well as audit requirements for other supporting functional requirements, is provided in ISO/IEC 15408 Part 2. Auditable events and transactions should be selected carefully such that important audit events are collected and can be analysed without being lost in excessive audit data. (578)

C.4.5.5 Cryptographic key management policy

Guidance

Cryptographic keys should be used and administered in a secure manner throughout their lifecycle. This encompasses cryptographic key generation, cryptographic key distribution, cryptographic key access (including backup, archival, and recovery) and cryptographic key destruction. (579)

ISO/IEC 15408 Representation

To specify the requirements of a cryptographic key management policy in a PP/ST, component(s) from the FCS_CKM (Cryptographic Key Management) family should be selected. (580)

The FCS_CKM family defines the requirements for the various cryptographic key management functions. If the TOE performs one or more of these cryptographic key management functions, appropriate component(s) from the FCS_CKM family should be selected. (581)

C.4.5.6 Physical security policy

Guidance

The requirements of the physical security policy, pertaining to the hardware and firmware comprising the TOE and the environment within which it is located, should be described in the PP/ST. (582)

The physical security policy should address the following aspects: (583)

a) The environmental assumptions (these should be the same as the general environmental assumptions for any PP/ST, whether it includes cryptography or not). These assumptions should typically be modelled as assumptions (see Chapter 3). However, if they directly refer to requirements on the software, firmware and/or hardware in the IT environment then they should be modelled as security requirements for the IT environment.

b) The responsibilities of the various classes of users and administrators for the physical protection of the TOE (this information should also be in the user and administrator guidance documents).

ISO/IEC 15408 Representation

Physical, procedural and personnel measures applied external to the TOE are typically expressed as assumptions. In addition, components from the following two assurance families should be selected. (584)

a) AGD_USR (User Guidance)

b) AGD_ADM (Administration Guidance)

Component(s) from the AGD_ADM family should be used to express the requirement to document the physical and environmental constraints under which the TSF should be operated by an administrator. (585)

Component(s) from the AGD_USR family should be used to express the requirement to document the physical and environmental constraints under which the TSF should be correctly operated by a user. (586)

If the TOE itself implements physical security requirements then component(s) from the FPT_PHP (TSF Physical Protection) family should be selected for inclusion in the PP/ST. These components can be used to express the physical security requirements to be placed on the TSF to prevent physical tampering or interference, as well as how to respond to such attacks. (587)

In the following example, instantiation of the FPT_PHP.2 component, expresses the physical security requirements for the protection of the hardware and firmware comprising the TOE. Component FPT_PHP.3 specifies the action taken to protect the cryptography-related IT assets if tampering is detected. (588)

FPT_PHP.2 Notification of physical attack

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF:

a) *The contents of the TSF shall be completely contained within a tamper detection envelope which will detect tampering by means such as drilling, milling or grinding of the TOE enclosure or cover.*

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices and TSF's elements has occurred.

FPT_PHP.2.3 For the devices/elements comprising the TOE, the TSF shall monitor the devices and elements and notify the user of the TOE when physical tampering with the TSF's devices and TSF's elements has occurred.

FPT_PHP.3 Resistant to physical attack

FPT_PHP.3.1 The TSF shall resist the following physical attack scenarios to the TSF's devices and TSF's elements by responding automatically such that the TSF is not violated:

a) The TOE shall be contained within a strong non-removable enclosure. The enclosure shall be designed such that attempts to remove or penetrate it will have a high probability of causing serious damage to the TOE (i.e., the TOE will not function).

b) If the TOE cover or enclosure contains any ventilation holes or slits, then they shall be small and constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or block with a substantial blocking material).

c) Upon the detection of tampering, all plaintext cryptographic keys and other unprotected critical security parameters shall be immediately zeroised.

C.4.5.7 Electromagnetic emanations policy

Guidance

The level of electromagnetic radiation emanated by the TOE should be limited in order to prevent the disclosure of cryptography-related IT assets to unauthorised individuals or users. In addition, procedural and physical measures should also be taken to prevent the detection of electromagnetic emanations by unauthorised individuals or users. Similarly, there may be physical shielding requirements relating to the prevention of electromagnetic interference (EMI)/radio frequency (RF) radiation from unwanted sources for integrity or availability reasons. (589)

However, the evaluation of technical physical aspects of IT security such as electromagnetic emanation control (e.g. TEMPEST) is not specifically covered by ISO/IEC 15408 (see [15408-1] clause 1, page 1, item b), although many of the concepts addressed will be applicable to that area. In particular, ISO/IEC 15408 addresses some aspects of physical protection of the TOE. (590)

ISO/IEC 15408 Representation

Organisational security policy statements (see Section C.3.2) should be used to define the electromagnetic emanation controls required for the TOE. (591)

Given that the evaluation of electromagnetic emanation requirements are explicitly excluded from ISO/IEC 15408, assumptions should be used to articulate the requirement for the TOE to implement that security policy. Assumptions should also be used to specify any procedural and physical measures that need to be taken to prevent the detection of electromagnetic emanations by unauthorised individuals or users, or to prevent unwanted EMI/RF radiation. (592)

C.4.6 TOE security functionality

C.4.6.1 Introduction

Security functionality required to implement aspects of the TOE security policy are addressed in the preceding section. This section addresses the remaining security functionality that is typically found in a TOE containing cryptographic functionality. (593)

In order to provide an effective and secure TOE containing cryptographic functionality, two types of security requirements typically need to be considered: (594)

a) the cryptographic functional security requirements;

b) other non-cryptographic functional and assurance security requirements that support that cryptographic functionality and the TOE security policy.

Discussion of how to express the TOE security policy using ISO/IEC 15408 is limited to Section C.4.5. (595)

C.4.6.2 Cryptographic functionality

Guidance

Cryptographic keys must be managed throughout their lifetime. The typical events in the lifecycle of a cryptographic key include (but are not limited to): generation, distribution, entry, storage, access (e.g., backup, archive, recovery) and destruction. (596)

As a minimum, cryptographic keys should at least go through the following stages: generation, storage and destruction. The inclusion of other stages is dependent on the key management strategy being implemented as the TOE need not be involved in all of the key life-cycle (e.g., the TOE may only generate and distribute cryptographic keys). (597)

The actual cryptographic functional security requirements can be considered as two distinct sub-types: (598)

a) functional security requirements for performing aspects of cryptographic key management, e.g.:

- cryptographic key generation;
- cryptographic key distribution;
- cryptographic key access;
- cryptographic key destruction.

b) functional security requirements for performing a cryptographic operation, e.g.:

- digital signature generation and/or verification;
- cryptographic checksum generation for integrity and/or for verification of checksum;
- secure hash (message or file digest) computation;
- data encryption and/or decryption;
- cryptographic key encryption and/or decryption;
- cryptographic key agreement.

As stated at the start of this annex, the scope of this guidance excludes the strength of cryptography, including key size and strength of algorithm. In fact, no ISO/IEC 15408 functional or assurance family (including AVA_SOF) may be used for the purposes of evaluating the strength of cryptographic functions or key sizes used. This is because ISO/IEC 15408 specifically does not cover the assessment of cryptographic algorithms and related techniques. Should independent assessment of the mathematical properties of cryptography embedded in the TOE be required, the scheme under which ISO/IEC 15408 is applied must make provision for such assessments. (See also [15408-1], clause 1, page 2, item e.) (599)

The implementation of the pseudo-random number generator is also critical to the security of cryptographic keys and cryptographic operations. The algorithm and parameters associated with pseudo-random number generators should be selected to optimise the degree of unpredictability as well as the size of the random number space. A strength of TOE security function claim (AVA_SOF) should be provided for the pseudo-random number generator implementation. (600)

ISO/IEC 15408 Representation

Depending on the cryptographic functions that the TOE performs, component(s) from the following families should be selected for inclusion in the PP/ST: (601)

a) FCS_CKM (Cryptographic Key Management)

b) FMT_MSA (Management of security attributes)

c) FCS_COP (Cryptographic Operation).

Note that the FCS class is organised into two families: FCS_CKM (Cryptographic Key Management) and FCS_COP (Cryptographic Operation). The FCS_CKM family addresses the management aspects of cryptographic keys, whilst the FCS_COP family is concerned with the operational use of those cryptographic keys. (602)

Component(s) from the FCS_CKM family can be used to specify functional requirements which implement the different aspects of the cryptographic key management policy. The family is intended to support the cryptographic key lifecycle and consequently defines requirements for cryptographic key generation, cryptographic key distribution, cryptographic key access and cryptographic key destruction. This family should be included whenever there are functional requirements for the management or administration of cryptographic keys. (603)

However, PP/ST developers should note that: (604)

a) The FCS_CKM family does not provide a specific component for protection of cryptographic keys while in storage. It is recommended that the components from the FDP_ACC (Access Control Policy) and FDP_ACF (Access Control Functions) families be used for the protection of user cryptographic keys stored in the TSF (i.e., stored as user data). The protection of TSF cryptographic keys (i.e., stored as TSF data) should be addressed by use of components from the FPT_SEP (Domain Separation) family or the FMT_MTD family. Note that either of the FDP or FPT classes may be used to ensure confidentiality and/or integrity of cryptographic keys.

b) The FCS_CKM family does not provide a specific component for protection of cryptographic key entry. Cryptographic keys may be entered in unencrypted, encrypted or split knowledge forms. A component from the FDP_ITC (Import from Outside TSF Control) family should be used to specify this requirement. If used, the assignment of “*additional importation control rules*” should be used to define whether the cryptographic keys need to be encrypted into split knowledge form or not.

c) Aspects of cryptographic protocol security should be expressed using components from the FCS_CKM family, and in particular those concerning cryptographic key distribution (FCS_CKM.2).

d) If public cryptographic keys need to be revoked, then the FCS_CKM.2 component should be used to specify public cryptographic key revocation. The reason FCS_CKM.2 is appropriate is that this component specifies cryptographic key distribution schemes, and distribution of revocation information is considered to be an integral part of cryptographic key distribution (e.g., as demonstrated in the X.509 standard for certificate revocation lists).

Component(s) from the FMT_MSA (Management of security attributes) family should be used to define cryptographic key attributes. Examples of key attributes include user, key type (e.g. public, private, secret), validity period, use (e.g. digital signature, key encryption, key agreement, data encryption). (605)

Component(s) from the FCS_COP family can be used to specify functional requirements which perform the cryptographic operations. Cryptographic operations may be used to support one or more TOE security services. The FCS_COP component may need to be iterated more than once depending on: (606)

a) the user application for which the security service is being used;

b) the use of different cryptographic algorithms and/or cryptographic key sizes; and/or

c) the type or sensitivity of the data being operated on.

If the TOE does not implement, or only implements part of, the cryptographic key management lifecycle, then any assertions placed on activities or components outside the TOE (i.e., in the TOE environment) should be expressed as assumptions. (607)

C.4.6.3 Import, export and inter-TSF transfer of cryptography-related IT assets

Guidance

Implicit to the implementation of the user access control policy, is the security of cryptography-related IT assets (such as unencrypted cryptographic keys, plaintext authentication data and other critical security parameters) being transmitted through intervening untrusted components or directly to/from human users. (608)

It is important that the users are aware of the sensitivity of this information and do not accidentally mix this information or its sensitivity with other information. Historically, cryptographic designers and implementers have achieved this by requiring a separate physical port for input and output of such information, thus making the users and the TOE aware of the sensitivity of the information. An alternative approach might be to use security labelling of data.(609)

ISO/IEC 15408 Representation

Component(s) from the following families should be selected: (610)

a) FDP_ITC (Import from Outside TSF Control)

b) FDP_ETC (Export to Outside TSF Control)

c) FTP_ITC (Inter-TSF Trusted Channel) or FTP_TRP (Trusted Path).

Element(s) from the FDP_ITC.2 component should be used to express the security requirement on the introduction of information into the TOE. It should be instantiated using the user access control SFP. (611)

Element(s) from the FDP_ETC.2 component should be used for specifying export rules for data from the TOE. It should be instantiated using the user access control SFP. (612)

Component(s) from the FTP_ITC family should be used to express the security requirement on the transfer of cryptographic assets between the TSF and the TSF of other TOE(s). Alternatively, component(s) from the FTP_TRP family can be used to express requirements for the input and output of cryptographic assets from/to human users. However, developers should note that use of the FTP_TRP and FTP_ITC families is mutually exclusive. (613)

For example: (614)

FTP_TRP.1 Trusted Path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and local users that is logically distinct from other communication paths and provides assured identification of its endpoints and protection of the communication data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit itself and the local users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication, and input and output of unencrypted cryptographic key components, plaintext authentication data, and other unprotected critical security parameters.

C.4.6.4 Maintaining a secure state

Guidance

Historically, the concerns over the design errors or malfunctions in a TOE containing cryptographic functionality have led to the following types of requirements being imposed: (615)

a) In order to prevent the inadvertent output of sensitive cryptographic information, two independent internal actions shall be required to output data via any output interface through which unencrypted cryptographic keys or other critical security parameters or sensitive data could be output.

b) When an error in the TOE is detected, the TOE shall enter the error state and suppress all output.

The intent of the first item is to make sure that an error in design or operation of the TOE does not accidentally release sensitive cryptographic information. (It also implies that the TOE can detect the release of sensitive cryptographic information.) The intent of the second item is that when the TOE detects an error, it should not release sensitive cryptographic information. In summary, in the event of an error occurring, the TOE should always aim to preserve a secure state. (616)

ISO/IEC 15408 Representation

Component(s) from the FPT_FLS (Fail Secure) family should be selected to express the requirement for the TOE to preserve a secure state whenever an error occurs. For example: (617)

FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur:

a) *The TOE incorrectly attempts to output unencrypted cryptographic keys, plaintext sensitive data, or other unprotected critical security parameters;*

b) *Failure of a cryptographic function;*

c) *Failure of TOE abstract machine tests (start-up, on demand and/or conditional);*

d) Detection of TOE physical tampering (including environmental failure).

This secure state shall mean that output is suppressed and no other functions are performed until the trusted recovery is performed.

PP/ST developers should note that this component has a dependency on the ADV_SPM.1 (Informal TOE security policy model) component. In addition, PP/ST developers will also need to include components to specify the functionality which may generate an error (e.g. the functionality to perform TOE self-testing). (618)

Component(s) from the FPT_RCV family may optionally need to be used to specify the requirement to return the TOE to a secure state and/or to prevent transition to an insecure state. (619)

C.4.6.5 Self-testing of cryptographic functions

Guidance

Implicit from the need for any TOE to preserve a secure state whenever an error occurs, is the need for functionality to detect that such errors have actually occurred. (620)

Typically, TOEs are designed to conduct self-tests on the cryptographic functionality to ensure that they are operating correctly. Such self-tests typically include: (621)

a) start-up (power-up or boot) self-tests:

  - known answer test;
  - software/firmware integrity test;
  - statistical random number generator tests.

b) on-demand tests:

  - known answer test;
  - software/firmware integrity test;
  - statistical random number generator tests.

c) conditions and conditional tests:

  - generation of private, public key pair, pair-wise consistency test;
  - software/firmware loading, software/firmware integrity check;
  - key entry, key integrity test;
  - random number generation, random number test.

ISO/IEC 15408 Representation

In order to specify the requirements for TOE self-testing, component(s) from one or more of the following families should be selected: (622)

a) FDP_SDI (Stored Data Integrity)

b) FPT_AMT (Underlying Abstract Machine Test)

c) FPT_TST (TSF Self Test).

Component(s) from the FDP_SDI family should be used to express the requirement to detect data integrity errors and to take remedial action (if any). (623)

Component(s) from the FPT_AMT family should be used to specify the tests to be performed on the underlying abstract state machine (e.g. on start-up, on demand and conditionally). (624)

Component(s) from the FPT_TST family should be used to express the requirement: to detect the corruption of cryptographic code by various failures that do not necessarily stop the TOE's operation, to test that the TSF is operating correctly (e.g. on start-up, on demand and conditionally). (625)

C.4.6.6 External dependencies

Guidance

In certain circumstances, the TOE may have dependencies on other software, firmware or hardware (e.g. on the security functionality of an underlying operating system). (626)

ISO/IEC 15408 Representation

As described in Chapter 5 to this Guide, SFRs that are expected to be satisfied by other software, firmware or hardware external to the TOE should be specified in the security requirements for the IT environment section of the PP or ST. (627)

C.4.7 TOE testing

C.4.7.1 Guidance

The functionality of the TOE should be tested to provide assurance that the TSF satisfies at least the SFRs that are specified. Testing requirements should therefore be selected based on the sensitivity of the application and their assurance needs. Attention should be paid to whether testing should be conducted by an independent third party, testing rigor and coverage, and the nature of TOE abstraction the rigor applies to (e.g., functional specification, high-level design, low-level design.) (628)

The vulnerability of the TOE to attack should also be analysed. (629)

C.4.7.2 ISO/IEC 15408 Representation

Component(s) from the following families should typically be selected: (630)

a) ATE_COV (Coverage)

b) ATE_DPT (Depth)

c) ATE_FUN (Functional testing)

d) ATE_IND (Independent testing)

e) AVA_VLA (Vulnerability analysis).

Component(s) from the ATE_COV family can be used to specify requirements for the completeness of the TOE testing. (631)

Component(s) from the ATE_DPT family can be used to specify requirements for the level of detail to which the TOE is tested. (632)

Component(s) from the ATE_FUN family can be used to specify requirements to establish that the TSF exhibits the properties necessary to satisfy the functional requirements identified elsewhere in the PP/ST (633)

Component(s) from the ATE_IND family can be used to specify requirements to demonstrate that the TSFs perform as specified. (634)

Component(s) from the AVA_VLA family can be used to specify requirements for environmental failure testing of a TOE containing cryptographic functionality. (635)

C.4.8 TOE operation

C.4.8.1 Guidance

Guidance should be provided for the secure installation, administration and operation of the TOE by its authorised users. (636)

C.4.8.2 ISO/IEC 15408 Representation

To express this requirement in the PP/ST, component(s) from the following families should be selected: (637)

a) AGD_ADM (Administration Guidance)

b) AGD_USR (User Guidance)

Component(s) from the AGD_ADM family should be used to express the requirement to document how the TOE should be correctly installed and administered by an administrator. (638)

Component(s) from the AGD_USR family should be used to express the requirement to document how the TOE should be correctly operated by a user. (639)

C.5 Guidance on applying assurance requirements

As previously stated, the scope of this document does not address the strength of cryptography, the choice of key size or the strength of any algorithm. However, whilst the choice or suitability of a cryptographic algorithm (and key size) is not within the scope of ISO/IEC 15408, the implementation of that algorithm in a TOE is within its scope. (640)

It is the responsibility of the sponsor of the TOE evaluation to select the algorithm(s), mode(s) and key size(s) that are used by the TOE. The sponsor may use one or more of the following approaches to ensure the correctness of the implementation: (641)

a) The sponsor may provide a compliant implementation.

b) The sponsor may vouch for the standard conformance of the implementation.

c) The sponsor may waive the conformance testing requirement.

d) The sponsor may conduct the conformance tests.

e) The sponsor may require the evaluators to conduct conformance tests. These tests shall be conducted using the conformance tests specified by the standard. If the standard does not specify conformance tests, the sponsor may provide or point to another source for the tests.

f) The sponsor may review the implementation (e.g., conduct a detailed code walk-through) in accordance with the ADV_RCR component.

g) The sponsor may require the evaluators to review the implementation (e.g., conduct a detailed code walk-through) in accordance with the ADV_RCR component.

It should be noted that the implementation review may be waived regardless of the ISO/IEC 15408 assurance level as the source code may not be available to the evaluators due to the sensitivity of the algorithm. The algorithm conformance testing may also have to be waived due to the lack of availability of conformance tests (this is especially true of new algorithms). (642)

Annex D Worked Example: Firewall PP and ST

This annex illustrates application of the guidance contained within Chapters 3 to 8 by means of a worked example based on a firewall. (643)

D.1 PP/ST Introduction

The PP and ST introductions were constructed following the guidance given in Chapter 3 of this Guide. The CC conformance claim in the ST stated that the ST was conformant with the PP as well as fully conformant with CC Part 2 and Part 3. (644)

D.2 TOE Description

The TOE Description section in the PP and ST were constructed following the guidance given in Chapter 3 of this Guide. In the case of the PP, a general description of the scope of the TOE and its security functionality was provided (since the TOE's sole purpose is security). More detail was provided in the ST, in particular: (645)

a) identifying the underlying operating system and hardware platform;

b) briefly describing the operating environment, e.g. in terms of the need for physical protection of the TOE, and the distinction between administrators of the firewall and users (who do not directly login to the firewall).

D.3 Security Environment

D.3.1 Assumptions

For a firewall, a number of assumptions can be identified as being necessary to ensure that the effectiveness of the firewall is not undermined. For example: (646)

a) The firewall is 'dual-homed': this is required since otherwise it would be possible to bypass the firewall altogether;

b) Only administrators can access the firewall: this assumption is necessary in order to limit the opportunities available to attackers.

Assumptions regarding the use of the security features (e.g. audit trail management and analysis) would be handled either as security objectives for the environment or as security requirements for the non-IT environment. (647)

D.3.2 Threats

For a firewall, the intended environment could be assumed to comprise a private network on one side of the firewall and an assumed hostile network on the other side. The IT assets to be protected are therefore the services provided by, and the information stored on the private network. The threat agents are, in general, *attackers on the hostile network*. (648)

An example threat to be countered by the firewall could be: (649)

> *An attacker on the hostile network may exploit flaws in service implementations to gain access to hosts or other services.*

This statement of threat follows the guidance given above in the following way: (650)

a) the threat agent is *an attacker on the hostile network*;

b) the IT assets subject to the attack are *hosts or other services* on the private network;

c) the form of the attack is denoted by *exploit flaws in service implementations*.

It should be noted that this threat statement does not contravene the guidance in referring to exploitation of flaws in service implementations (such as ‘sendmail’) since these are not part of the TOE itself (although the relevant application proxies are). (651)

Although most of the threats to be addressed by the firewall are posed by *attackers on the hostile network*, it is possible that one could identify a threat as follows, where the *attacker* could be either on the hostile network or the private network: (652)

> *An attacker may gain access to the firewall by impersonating an administrator*

This particular threat is included as a result of the firewall being introduced into the intended environment. It should be noted that (in line with the guidance stated above) it does not presume anything concerning the countermeasures provided by the TOE, other than assuming that the effectiveness of the firewall in countering the threats is, to some extent, dependent on the identified administrator of the firewall. (Note that the ‘personnel’ section of the assumptions would indicate the existence of such a role and the general responsibilities that go with it). (653)

The threats identified as not being countered by the TOE reflect the practical limitations on the firewall. For example: (654)

a) Specific attack methods posed by attackers on the hostile network that are not countered by the TOE, such as session hi-jacking and data sniffing.

b) The private network may be made vulnerable to attack as a result of actions taken by hostile users on the private network.

c) The vulnerability of the private network to viruses which could be contained within incoming traffic, a threat which the firewall is not designed to counter.

d) The private network could be made vulnerable to attack as a result of action or inaction by the firewall administrator.

e) The private network could be made vulnerable to attack as a result of physical attack on the firewall itself.

A possible (and particularly interesting) threat for an application gateway firewall would be: (655)

> *Attackers on the hostile network exploiting new, previously unknown, attack methods e.g. using previously trustworthy services.*

This recognises that the threat posed by attackers on the hostile network is dynamic (i.e. continually changing), and the fact that the TOE itself may need to change, e.g. by providing proxies for new applications. (656)

D.3.3 Organisational Security Policies

In general, a firewall will be capable of being configured to implement a number of different organisational security policies. For this example, it is therefore possible that little would be gained from specifying the organisational security policies with which the TOE should comply. However, it might be possible to state in general terms the access control policy to be implemented by the firewall. (657)

D.4 Security Objectives

D.4.1 Security Objectives for the TOE

The security objectives for a firewall could be specified as follows: (658)

a) The principal security objective would be for the firewall to enforce access control, for example in terms of limiting the valid range of addresses, and the hosts and service ports that can be accessed.

b) The provision of ‘sanitised’ servers to counter the threat of vulnerabilities in service implementations may be a security objective for an application gateway firewall.

c) Similarly, there may be a security objective for application proxy authentication.

d) A security objective for audit, providing a means of recording security relevant events.

e) A security objective for security administration, both in terms of the functions that must be available to administrators, and also in terms of controlling access to that functionality.

An example security objective for the TOE would be: (659)

> *The firewall must, for certain specified services on the private network, be capable of requiring authentication of the end user prior to establishing a through connection.*

This acts as a clear pointer to the need for the TOE to provide Identification and Authentication functionality. It may be noted that because the PP does not identify the services that must be provided, the security objective does not identify the subset of those services which require authentication. This is left as an issue for the ST author who (in the ST rationale) must justify those services that require (or can be configured to require) authentication of the end user. (660)

D.4.2 Security Objectives for the Environment

An example of a security objective for the environment is the following, which relates to the usage of audit functionality: (661)

> *Administrators of the firewall must ensure that audit facilities are used and managed effectively. In particular, appropriate action must be taken to ensure continued audit logging, e.g. by regular archiving of logs to ensure sufficient free space. Furthermore, audit logs should be inspected on a regular basis and appropriate action should be taken on the detection of breaches of security, or events that are likely to lead to a breach in the future.*

This security objective is therefore closely linked with the security objective for the firewall to provide auditing functionality. (662)

D.5 IT Security Requirements

D.5.1 Security Functional Requirements

Following the guidance described in Chapter 5, the following SFRs might be selected to directly meet the security objectives for the TOE, as described in the previous section: (663)

a) The security objective requiring the firewall to enforce an access control policy based on the apparent target host or service, or the apparent source host or service, could be satisfied by suitable use of either FDP_IFF.1 (Simple Security Attributes) and FDP_IFC.2 (Complete Information Flow Control), or by FTA_TSE.1 (TOE Session Establishment).

b) The security objective requiring the firewall to provide application proxy authentication could be satisfied by FIA_UAU.2 (User Authentication Before Any Action) and FIA_UID.2 (User Identification Before Any Action). Other SFRs suitable for consideration include FIA_UAU.3 (Unforgeable Authentication), FIA_UAU.4 (Single-use Authentication Mechanisms) and FIA_UAU.5 (Multiple Authentication Mechanisms), as these allow for the specification of stronger authentication mechanisms.

c) The security objective requiring the provision of audit functionality could be satisfied by FAU_GEN.1 (Audit Data Generation) and FAU_ARP.1 (Security Alarms) to provide more real-time audit analysis.

d) The security objective requiring the provision of security administration functionality may be satisfied by FMT_SMR.1 (Security Management Roles), together with FIA_UAU.2 and FIA_UID.2 applying to authentication of the firewall administrator.

Having selected the initial set, the remaining SFRs would be selected mainly to satisfy ISO/IEC 15408 Part 2 dependencies. Additional SFRs could be included because they provide a useful (if not essential) supporting role; examples may include FIA_AFL.1 (Authentication Failure Handling), FPT_RVM.1 (Non-bypassability of the TSP) and FPT_SEP.3 (Complete Reference Monitor). (664)

A further decision to be made concerns the level of audit (i.e. *not-specified, minimum, basic* or *detailed).* The appropriate level will be chosen so as to be sufficient to meet the security objectives for the TOE whilst at the same time not stipulating an unduly onerous set of security requirements. For example, if FTA_TSE.1 (TOE Session Establishment) is the component used to specify the firewall access control policy, then a *basic* level of audit may be appropriate as this requires successful and unsuccessful attempts to be logged (not required by the *minimal* level of audit). Alternatively, *not specified* could be chosen, and the specific auditable events selected as considered appropriate for the threats. (665)

Assignments will be completed in the firewall PP for the purposes of clarity where necessary. For example: (666)

a) the selection *success or failure* would be made in FAU_GEN.1.2 since this is an explicit requirement of the audit security objective;

b) the selection *an authorised administrator configurable number* would be made in FIA_AFL.1.1 to permit flexibility in the choice of the number of unsuccessful authentication attempts, in accordance with local security policy;

c) the assignment *application proxy authentication* would be made in FIA_AFL.1.1 to make it clear that the SFR applies to this type of authentication, and not that of the firewall administrator (which would probably be an undesirable security requirement).

D.5.2 Assurance Requirements

The selection of the assurance requirements should be relatively straightforward. If the PP or ST authors have identified (in the security objectives) no need for specific assurance requirements, selection may simply boil down to the choice of an appropriate EAL. For example, the nature of the threat (including relatively sophisticated attacks) and the value of IT assets to may point to EAL4 as a suitable choice, taking into account also the likely assurance level achievable by existing TOEs for which a claim of compliance might be made. (667)

D.5.3 Security Requirements on the IT Environment

The firewall itself will not necessarily provide all of the functionality needed to satisfy the security objectives for the TOE. For example, the firewall could legitimately rely on the underlying operating system to provide for storage of the firewall audit trail. The PP authors will therefore need to come to a judgement as to which functionality was required of the firewall in all cases, and which could, optionally, be provided by the underlying operating system. (668)

The appropriate approach to take would be to include, in the minimum set of functions to be provided by the firewall, all SFRs identified as directly providing the security objectives for the TOE. Other security requirements, included in the PP to (for example) satisfy ISO/IEC 15408 Part 2 dependencies, could be placed in the security requirements for the IT environment section where this appeared sensible. (669)

For example, security requirements for the protection of the stored audit trail (e.g. FAU_STG.1) could be placed on the IT environment, together with associated security requirements for review of the audit trail (e.g. FAU_SAR.1). However, SFRs (specified using FMT_MSA.1) that are associated with the management of security attributes relating to the *primary* SFRs might be placed on the firewall. (670)

Similarly, although the security objectives for the TOE indicate a need to authenticate administrators, the PP could permit this functionality to be provided by the underlying operating system. This is not unreasonable since the fundamental security objective to be met is that it must be ensured that only the authorised administrator can exercise administrative control over the firewall. Authentication of administrators may be regarded as a means by which this security objective can be met. (671)

Selection of the assurance requirements is straightforward in this case, being governed by the TOE security assurance requirements, e.g. EAL4. (672)

D.6 TOE Summary Specification

D.6.1 IT Security Functions

In constructing the IT security functions, the ST authors could begin with the SFRs and derive IT security functions from these in the following way: (673)

a) TOE specific details would be added where appropriate to clarify the functionality, particularly for the firewall access control functions (these representing the main purpose of the TOE);

b) For supporting functions (particularly security management functions), attempts would be made to make the functions more concise, without losing essential detail; in some cases this led to a combination of one or more functional requirements in a single security function.

An example of the first is as follows: (674)

The TOE will control access on the basis of:

- *apparent source IP address or host name*
- *apparent source port number*
- *destination IP address or host name*
- *destination port number.*

An example of the second is as follows: (675)

The firewall administrator, and only the firewall administrator, can perform the following functions:

- *display and modify the firewall access control parameters*
- *initialise and modify user authentication data*
- *display and modify user attributes*
- *select events to be audited*
- *identify the subset of auditable events deemed to indicate a possible or imminent security violation*
- *associate separate authentication mechanisms with specific authentication events*
- *verify the integrity of the firewall.*

In this way, it would be possible to encapsulate the requirements of several SFRs in a single IT security function (the SFRs would need to be specified using FMT_MSA.1.1, FMT_MOF.1.1, FMT_MTD.1.1 and FPT_TST.1.3). Note, however, that the scope for achieving a more concise statement of security functions in this area would be reduced for TOEs implementing multiple administrator roles. (676)

D.7 PP Rationale

D.7.1 Security Objectives Rationale

The demonstration of the suitability of the security objectives to counter the threats may be provided by: (677)

a) showing, by means of a table, which security objectives counter which threats (e.g. O.ACCESS, which defines the need for a firewall access control policy may be correlated with the threats posed by attackers on the hostile network such as IP spoofing or attacks on vulnerable services), ensuring that each security objective is mapped onto at least one threat;

b) providing, for each threat, an argument as to why the identified security objectives were suitable to counter the threat.

An example of the justification of suitability is given below: (678)

T.PROTOCOL An attacker on the hostile network may exploit inappropriate use of service protocols (e.g. using a 'well known' port number for a protocol other than the one defined to use that port.

O.ACCESS limits the hosts and service ports that can be accessed from, respectively, the hostile and private networks. O.AUDIT monitors possible attacks, providing the firewall administrator with the means of detecting them, and hence taking appropriate action. O.ADMIN provides essential support by ensuring secure administrative control of the firewall, supported by O.INSTALL and O.TRAIN.

D.7.2 Security Functional Requirements Rationale

The demonstration of the suitability of the SFRs to satisfy the security objectives for the TOE may be provided by: (679)

a) showing, by means of a table, which SFRs satisfy which security objectives (e.g. FDP_ACF.1 and FDP_ACC.2 may be correlated with O.ACCESS), ensuring that each SFR is mapped onto at least one security objective;

b) providing, for each security objective for the TOE, an argument as to why the identified SFRs are suitable to satisfy the security objective.

An example of the justification of suitability is given below: (680)

O.ADDRESS The firewall must limit the valid range of addresses expected on each of the private and hostile networks (i.e. an external host cannot spoof an internal host).

FDP_ACF.1 together with FDP_ACC.2 provides the capability of limiting access in the manner required by O.ADDRESS, and FPT_RVM.1 ensures that these functions are always invoked when required.

The demonstration of mutual support and internal consistency may be provided firstly by means of a dependency analysis, following the guidance in Chapter 7. This may then be supplemented by a table showing how each SFR is protected against bypassing, tampering and de-activation attacks by other SFRs. This may be followed by an explanation of the table contents. Rather than taking each SFR in turn (which would have led to a repetitive discussion), the general issues can be highlighted so that the table contents could be understood. For example: (681)

Tampering attacks are prevented by:

- *FPT_SEP.3 which maintains domain separation, and in particular prevents an attacker from tampering with the security functions;*
- *Security functions which restrict the modification of attributes or configuration data to the authorised administrator (e.g. those based on FMT_MSA.1);*
- *Security functions which prevent the unauthorised modification of other data, the integrity of which is critical to a security function (i.e. those based on FMT_MTD.1).*

D.7.3 Assurance Requirements Rationale

The construction of this part of the PP Rationale should relatively straightforward if the PP (for example) mandates EAL4 and does not specify any augmented assurance requirements. In this event it would be possible to assert that EAL4 provides a known set of mutually supportive and internally consistent assurance components, for which all assurance dependencies are satisfied. (682)

The justification for the choice of EAL may be provided as follows: (683)

a) it may be argued that EAL4 was necessary as being the lowest EAL for which the evaluators have access to the low level design and source code, such access being necessary to provide confidence that the TOE provided defence against sophisticated attacks as indicated in the TOE Security Environment section;

b) it may be argued that EAL4 is achievable for this type of TOE since it requires no specialist techniques on the part of the developer.

D.8 ST Rationale

For an ST produced to comply with the firewall PP, the ST rationale may make extensive reuse of the PP rationale. In particular: (684)

a) If the threats, organisational security policies, assumptions and security objectives are identical, then the Security Objectives Rationale in the ST will be identical to that given in the PP; hence this part of the ST rationale may simply refer to the relevant section in the PP rationale.

b) If the ST adds a small number of SFRs to those defined in the PP, the ST rationale may refer to the relevant part of the PP rationale, and show why:

- the additional requirements were suitable to satisfy the security objectives
- the additional requirements introduced no conflict, but were supportive of the other requirements
- the additional dependencies were satisfied or did not need to be satisfied

c) If identical security assurance requirements were specified in the ST, the Assurance Requirements Rationale may simply refer to the relevant part of the PP rationale.

This leaves the following aspects to be covered by the ST rationale: (685)

a) Justification of compliance with the PP. This may be done through use of a table to demonstrate coverage of all PP SFRs, and a second table showing how the appropriate PP operations are completed in the ST.

b) IT Security Functions Rationale. This may be done by explicitly linking the specified IT security functions with the SFRs. If no new functionality is introduced at this level, the demonstration of mutual support may be deemed to be provided by the Security Requirements Rationale.

Annex E Worked Example: Database PP

This annex illustrates application of the guidance contained within Chapters 3 to 8 by means of a worked example based on a database management system (DBMS). In this example, the DBMS is intended for use in commercial environments where there is a need to protect the confidentiality, integrity and availability of the information held in the database on a discretionary basis. (686)

E.1 TOE Security Environment

E.1.1 Assumptions

For a database, it is important that the statement of assumptions about the TOE security environment clearly establishes the scope and boundary of the TOE. A number of the assumptions that are identified as necessary to ensure that the effectiveness of the database is not undermined will be placed on the underlying platform (typically, an underlying operating system). For example, the following general assumptions may be made: (687)

A1 *The TOE relies on an underlying operating system that is assumed to be installed and operated in a secure manner, i.e. in accordance with the security target and guidance documents for the relevant product.*

A2 *The processing resources of the TOE and the underlying operating system are assumed to be protected from unauthorised physical access.*

A more specific assumption is that the database files, executables, and so on, that are stored by the underlying operating system are adequately protected, so that the security functions implemented by the database cannot be circumvented by authorised users of the operating system. This assumption may be stated as follows: (688)

A3 *All of the database-related files and directories are assumed to be protected from unauthorised access by the underlying operating system.*

It is important to remember that, at this point in the PP, the main concern is to establish the scope of the security needs to be addressed by the TOE itself, and which aspects are to be satisfied by the underlying operating system. The security objectives and requirements on the underlying operating system (as part of the IT environment) are specified later in the PP. (689)

As described in chapters 3 and 4, assumptions regarding the use of the security features (e.g. audit trail management and analysis) would be handled as security objectives for the environment. (690)

E.1.2 Threats

For a database, the IT assets to be protected are the database objects, and in particular the data contained within those objects. Database objects may comprise aggregations of data contained in other database objects. The confidentiality, integrity and availability of the information stored in those objects needs to be protected in accordance with the wishes of the owner of the database objects. (691)

The threat agents include authorised and unauthorised users of the database. The latter category includes both authorised and unauthorised users of the underlying operating system. (692)

An additional potential source of threats to the integrity and availability of the information held in the database are external events such as interruptions to operations arising from failures of hardware, power supplies, storage media, and so on. (693)

The two principal threats of unauthorised access to information held in the database can be represented as follows: (694)

T1 *An attacker gains access to the database as a result of impersonation of an authorised database user, or as a result of anonymous access.*

T2 *An authorised database user accesses information contained within a database without the permission of the user who owns or who has responsibility for protecting the data.*

These threat statement follows the guidance given in chapter 3 in the following way: (695)

a) the threat agent is *an authorised database user* in T2, but could be an unauthorised *or* an authorised database user in the case of T1;

b) the IT assets subject to the attack (in both threats) are the information held in the database objects being accessed;

c) the form of the attack is denoted by *impersonation* or *anonymous access* in T1, and by *accesses information* in T2.

The need to protect the availability of the information held in the database might give rise to the following threat: (696)

T3 *An authorised database user consumes global database resources in a way which compromises the ability of other authorised users to access the database.*

It should be noted that in threat T3 the IT asset at risk is still the information held in the database; the ‘global database resources’ are simply the means of executing the attack on the availability of database information. (697)

The threats identified as not being countered by the TOE reflect the practical limitations on the DBMS. For example: (698)

TE1 *The database cannot be reliably protected by the TOE from highly trusted users who abuse the privileges they are granted.*

This acts as a caveat on the general threat of abuse of privilege by an authorised user, for which security audit is the usual countermeasure. Clearly, there will be some trusted users who have sufficient privilege to be able to delete audit records, and thus ‘cover up their tracks’. This places the onus on the establishment of appropriate procedural measures to ensure highly trusted users are indeed trustworthy individuals. Threat TE1 will therefore give rise to a security objective for the environment to address this need. (699)

E.1.3 Organisational Security Policies

Although not the PP is not targeted for use by specific organisations, it is still possible to state the general access control policy that a compliant TOE should be capable of implementing (which may not be obvious from the statement of threats). For example: (700)

P1 Access rights to specific database objects are determined by:

a) the owner of the object;

b) the identity of the subject attempting the access;

c) the access rights to the object granted to the subject;

d) the privileges held by the subject.

E.2 Security Objectives

E.2.1 Security Objectives for the TOE

Security objectives for a DBMS could be specified as follows to address the threats T1, T2 and T3 identified above: (701)

O1 The TOE system must provide the means of identifying users of the TOE.

O2 The TOE must provide end-users with the capability of controlling and limiting access by identified individuals to the database objects they own or are responsible for, in accordance with the P1 security policy.

O3 The TOE must provide the means of controlling the consumption of global resources by specified users of the TOE, including the number of concurrent sessions.

These can be seen to address the relevant threats and the referenced OSP directly. O1 is particularly interesting since it is based on the assumption that the claimed identity of a user of the TOE is authenticated by the underlying operating system, which is part of the IT environment. The need for identification and authentication by the underlying operating system would be expressed as a security objective for the *environment*. (702)

E.2.2 Security Objectives for the Environment

Threat TE1, identified in section E.1.2 above, identified the need for a security objective for the environment relating to highly trusted users. This could be reflected in the following security objective: (703)

OE1 Those responsible for the TOE must ensure that adequate procedural and personnel measures are established and implemented to ensure that only highly trusted individuals are assigned user privileges which allow them to:

a) modify audit data or the audit configuration;

b) *modify user security attributes (including authorising use of user privileges).*

A further example of a security objective for the environment is the following, which applies to the use of the underlying operating system: (704)

OE2 Those responsible for the TOE must ensure that the authentication data for each user account for the underlying operating system is held securely and is not disclosed to individuals not authorised to use that account.

This is identified as a necessary security objective given the need (expressed in the assumptions described in section E.1.1 above) to ensure that database files are adequately protected by the underlying operating system: if the authentication data is not itself protected, an attacker may be able to circumvent these access controls. (705)

E.3 IT Security Requirements

E.3.1 Security Functional Requirements

Following the guidance described in Chapter 5, the following SFRs might be selected to directly meet the security objectives for the TOE, as described in the previous section: (706)

a) The security objective O1, requiring identification of users by the TOE (authentication is enforced by the underlying operating system), can be satisfied by SFRs specified using FIA_UID.1 (Timing of Identification) and FIA_USB.1 (User-Subject Binding).

b) The security objective O2, requiring enforcement of access control on database objects, can be satisfied by SFRs specified using FDP_ACC.1 (Subset Access Control) and FDP_ACF.1 (Security Attribute Based Access Control).

c) The security objective O3, requiring restrictions on the consumption of global resources, can be satisfied by SFRs specified using FRU_RSA.1 (Maximum Quotas) and FTA_MCS.1 (Basic Limitation on Multiple Concurrent Sessions).

In a similar way, the other security objectives included in the PP would be satisfied by selection of appropriate ISO/IEC 15408 Part 2 components to specify the required SFRs (e.g. FAU_GEN.1 to specify auditing requirements). (707)

Having selected the initial set, the remaining SFRs would be selected to satisfy ISO/IEC 15408 Part 2 dependencies or to identify other supporting functionality. For example: (708)

a) FMT_MSA.3 (Static Attribute Initialisation) is needed (as a dependency of FDP_ACF.1) to specify controls over the default protection on newly created database objects.

b) FMT_MSA.1 (Management of Security Attributes) is needed to specify controls over the modification or assignment of user security attributes and object security attributes. For clarity, the iteration operation would need to be used to specify the controls over user and object attributes separately, since the latter may be modified by the object owner, but the former by an authorised administrator only.

c) FDP_RIP.1 (Subset Residual Information Protection) would be used to specify object reuse functionality in support of the database access control policy.

d) FAU_SAR.1 (Audit Review) might be selected to specify who can review the audit data (for example, authorised users may be able to read audit records relating to the objects they own, whereas only an authorised administrator would be able to view the entire audit trail).

A further decision to be made concerns the level of audit (i.e. *not-specified, minimum, basic* or *detailed).* The appropriate level will be chosen so as to be consistent with the security objectives for the TOE, ensuring at the same time that the audit requirement is not unduly onerous. In practice, if none of *minimum*, *basic* or *detailed* is considered appropriate given the threats and security objectives, the *not-specified* level will be selected, and the set of auditable events chosen appropriately. (709)

Completed operations in the PP will be italicised for the purposes of clarity. For example: (710)

FMT_MSA.3.1 The TSF shall enforce the *database object access control policy* to provide *restrictive* default values for object security attributes that are used to enforce the *database object access control policy.*

FMT_MSA.3.2 The TSF shall allow *no users* to specify alternate initial values to override the default initial values when an object is created.

E.3.2 Assurance Requirements

As described in Chapter 5, the assurance requirements should be derived based on consideration of the nature of the threat constrained by what is technically feasible. For a DBMS targeted for use in commercial environments, an assurance requirement of EAL3 would be appropriate. As described in [15408-3], subclause 6.2.3, page 58, EAL3 provides a moderate level of assurance without requiring substantial re-engineering of the TOE (such a level is, for example, commensurate with a TCSEC C2 level of assurance). (711)

E.3.3 Security Requirements on the IT Environment

For a database TOE, this section is highly significant. The need for the underlying operating system to provide access control and (potentially) identification and authentication functionality has already been identified in the statement of security objectives. This suggests that an operating system which provides C2-like functionality (e.g. evaluated as compliant with a C2 PP) would be appropriate, and that therefore this section of the PP should require compliance with an appropriate PP or functional package. (712)

However, it should be borne in mind that a PP is intended to be generic, and that whereas C2-compliance (or equivalent) would be one way of satisfying the security requirements on the IT environment, it is not necessarily the *only* way of meeting them. Since ISO/IEC 15408 does not mandate the use of ISO/IEC 15408 Part 2 components to specify the security requirements, it is acceptable to define them in a more abstract manner, such that the essential security requirements are included without mandating C2-compliance. The ST for a compliant TOE may then demonstrate how these security requirements are satisfied by the underlying operating system(s) on which the TOE is to be evaluated. (713)

Specific security requirements may be identified as a result of satisfying the dependencies of SFRs provided by the TOE. For example, FAU_GEN.1 is dependent on FPT_STM.1 for the provision of timestamps; this functionality might be provided by the underlying operating system rather than the database. (714)

The assurance requirements on the IT environment must be at least equal to that of the compliant TOE, i.e. EAL3 in this case. (715)

E.4 PP Rationale

E.4.1 Security Objectives Rationale

The demonstration of the suitability of the security objectives to counter the threats may be provided by following the guidance given in Chapter 7, that is: (716)

a) showing, by means of a table, which security objectives counter which threats (e.g. T3 is addressed by O3), ensuring that each security objective is mapped onto at least one threat;

b) providing, for each threat, an argument as to why the identified security objectives were suitable to counter the threat.

An example of the justification of suitability is given below: (717)

> *T3 (Excessive Consumption of Resources) is countered directly by O3, which ensures that the TOE has the means of limiting the consumption of such resources, including the enforcement of limits on the number of concurrent sessions an individual user may have. O1 provides support by providing the means of identifying the user attempting to use resources. O4 provides support by controlling access to administrative functionality that might otherwise enable circumvention of resource utilisation controls.*

E.4.2 Security Functional Requirements Rationale

The demonstration of the suitability of the SFRs to satisfy the security objectives for the TOE may be provided by: (718)

a) showing, by means of a table, which SFRs satisfy which security objectives (e.g. FRU_RSA.1 and FPT_MCS.1 address security objective O3), ensuring that each SFR is mapped onto at least one security objective;

b) providing, for each security objective for the TOE, an argument as to why the identified SFRs are suitable to satisfy the objective.

An example of the justification of suitability is given below: (719)

> *O3 is provided by FRU_RSA.1, which provides the means of controlling the consumption of global resources by individual users, and by FTA_MCS.1, which provides the means of controlling the number of multiple concurrent sessions a user may have. These are supported by FIA_ATD.1, which provides the appropriate user security attributes permitting the definition of quotas, in conjunction with FIA_USB.1 which associates these attributes with subjects acting on the user's behalf.*

The dependency analysis may be provided by means of a table, in the manner described in the guidance in Chapter 7. (720)

The demonstration of mutual support and internal consistency may be provided by identifying and discussing the additional supportive dependencies between the identified SFRs (including, where appropriate, security requirements on the underlying operating system) not highlighted in the dependency analysis. This should be constructed by considering each SFR in turn and the potential need for other SFRs to prevent it from being bypassed or tampered with. Examples include: (721)

a) FDP_RIP.1 supports FDP_ACC.1 and FDP_ACF.1 by preventing these SFRs from being bypassed when storage objects are reused and accessed by different subjects.

b) FMT_MSA.1 supports FRU_RSA.1 and FTA_MCS.1 by restricting the ability to change user quotas to the authorised administrator, thus ensuring that other users cannot circumvent these SFRs.

c) FAU_STG.1 supports FAU_GEN.1 by protecting the integrity of the audit trail.

E.4.3 Assurance Requirements Rationale

The construction of this part of the PP Rationale should relatively straightforward if the PP (for example) mandates EAL3 and does not specify any augmented assurance requirements. In this event it would be possible to assert that EAL3 provides a known set of mutually supportive and internally consistent assurance components, for which all assurance dependencies are satisfied. (722)

The justification for the choice of EAL may be provided along the lines described in section E.3.2 above. (723)

Annex F Worked Example: Trusted Third Party PP

This annex illustrates application of the guidance contained within Chapters 3 to 8 by means of a worked example based on a Trusted Third Party (TTP). In this example, there is a need for flexibility in that the SFRs will be dependent on the types of services provided by the TTP. For example: (724)

a) the TTP may or may not provide confidentiality services;

b) the TTP may provide a key generation service, or may assume that the TTP subscribers have this capability themselves.

This consideration leads to the notion of defining a set of *core services* which a TTP *must* provide, together with a set of *supplementary services* which a TTP can optionally provide. The core services represent the minimum services expected of a TTP, relating to subscriber registration, and generation, distribution, revocation and archive of public authentication key certificates. TTP supplementary services include such things as key generation, certificate verification, and confidentiality services such as confidentiality key certificate management, key recovery and key escrow[1]. (Implicit within this division between core and supplementary services is the assumption that TTP subscribers will usually have their own applications to perform such functions as key generation, digital signature generation and verification, and so on.) (725)

This, however, creates a problem with respect to compliance with ISO/IEC 15408, since ISO/IEC 15408 does not permit the specification of optional security requirements in a PP. The alternative approach of producing a PP for every possible combination of TTP services was, given the multitude of possible permutations, considered impractical. (726)

The solution to this problem was therefore to define a core set of SFRs in the PP needed to support the secure provision of the TTP core services. In addition, for each identified supplementary service, a functional package was defined to identify the additional SFRs needed to support that service. The resultant TTP PP could then be used as follows: (727)

a) An ST for a specific TTP demonstrates compliance with the TTP PP by satisfying the core SFRs. The ST may also (optionally) claim compliance with one or more of the defined functional packages, dependent on the services provided by the TTP.

b) The TTP PP could also be used as the basis for generation of other PPs for a specific set of TTP services; such a PP would be based on combination of the core set of SFRs with one or more of the defined functional packages as appropriate. This could lead to a ‘family’ of TTP PPs.

[1] For the purposes of this example, key recovery is considered to be distinct from key escrow. In the former case, only the TTP subscriber can request recovery of his or her keys. In the latter case, another party (e.g. a law enforcement agency) may have the right to request TTP subscriber keys.

F.1 TOE Security Environment

F.1.1 Assumptions

For a TTP, it is important that the statement of assumptions about the TOE security environment clearly establishes the scope and boundary of the TOE. In this example, subscriber applications used to generate digital signatures or to encrypt or decrypt information are considered to be *outside* the boundary of the TOE. This leads to the following two assumptions. (728)

A.ALGORITHM *It is assumed that the TTP will not certify a public key if it is not satisfied of the integrity of the algorithm to which the key pair relates.*

A.SUBSCRIBER *It is assumed that subscribers have technical means available whereby they can (where needed) generate their own public/private key pairs, generate and verify digital signatures, and verify public key certificates.*

The first assumption is necessary because the certificate issued by the TTP would be devalued if there was no trust in the subscriber's implementation of the relevant algorithm. (729)

The second assumption is needed for completeness. A TTP could uphold this assumption by providing the relevant supplementary services. Otherwise, the assumption is that the capability is provided by subscriber applications that are outside the scope of the TOE. (730)

F.1.2 Threats

For a TTP, the IT assets to be protected are the certificates generated or stored (e.g. archived) by the TTP, together with keys used or generated by the TTP. Public keys and certificates, by their very nature, do not have any needs for protection of confidentiality; however integrity and availability are legitimate concerns. Private or secret keys, on the other hand, require protection against unauthorised disclosure. These may be keys used by the TTP to sign certificates, or subscriber keys generated or stored (for recovery or escrow) by the TTP. (731)

These assets ultimately derive value from the information exchanged by subscribers, which the keys and certificates are used to protect. The information itself is not within the scope of control of the TTP, but the keys and certificates are. A less tangible asset is the reputation of the organisation operating the TTP itself; again, this asset may be damaged by threats to the keys and certificates. (732)

The threat agents include TTP subscribers and authorised users of the TOE, as well as malicious individuals who have access to the TTP environment, or who may be able to engage in communications with the TTP. (733)

An example threat relevant to the TTP core services are as follows: (734)

T.AKEYREVEAL *A subscriber's private authentication key is revealed to an individual who has no legitimate need to know.*

This threat statement follows the guidance given in Chapter 3 in the following way: (735)

a) the threat agent is *an individual who has no legitimate need to know the subscriber's private authentication key*;

b) the IT asset subject to the attack is the *subscriber's private authentication key*;

c) the form of the attack is indicated by the wording *is revealed to*: this indicates that either passive or active attack is relevant (this would be expanded upon in an accompanying explanation of the threat).

A second example relates to the availability of public authentication key certificates: (736)

T.ACERTAVAIL *One (or more) public authentication key certificates managed by the TTP cannot be distributed or delivered to a subscriber who has a legitimate need to know.*

In the above threat specification, the asset at risk is clearly the *public authentication key certificates*. However, the threat agent and the method of attack are not explicit. In this case it is down to the accompanying explanation of the threat to identify the possible sources of the threats (e.g. failure of the TOE itself or of the TTP-subscriber communications path) and any relevant attack methods (this might include deliberate attempts at denial of service, or there may be no explicit attack involved if the source of the threat is an operational error in the TOE). (737)

Threats are also identified which are relevant only to specific TTP supplementary services. For example: (738)

T.CKEYAVAIL *One (or more) subscriber confidentiality keys cannot be distributed or handed to an individual who has a legitimate need to know.*

This threat is relevant to where a key recovery service is provided. It is also relevant if a key escrow service or confidentiality key generation service is provided by the TTP. (739)

No threats were identified as not being countered by the TOE. This is because potential threats to the assets are explicitly excluded by the assumptions made relating to the TOE security environment. (740)

F.1.3 Organisational Security Policies

Although not the TTP PP is not targeted for use by specific organisations, there may rules governing the TTP which are imposed by national legislation. The following OSP highlights the possibility; although such a general security policy requirement will have little tangible effect on the identified 'security solution', it will be expanded upon in a PP or ST that is based on the TTP PP. (741)

P.LEGAL *The TTP is required to conform to any applicable information security legislation.*

F.2 Security Objectives

F.2.1 Security Objectives for the TOE

Security objectives for the TTP are divided into core and supplementary service security objectives. Examples of the former are: (742)

O.CERTMANAGE *The TOE must provide the means to generate, distribute and revoke public key certificates in a timely manner.*

O.CERTVERIFY *The TOE must provide the means to verify public key certificates, which involves the verification of a chain of certificates to a trusted point.*

O.SIGNATURE *The TOE must provide the means to generate digital signatures as proof of origin.*

The first two, O.CERTMANAGE and O.CERTVERIFY, directly relate to core TTP services provided to the TTP subscribers. By contrast, O.SIGNATURE is not a core TTP service, but is nonetheless a security objective which must be satisfied in support of provision of the core service of certificate generation (i.e. TTPs must have the capability of signing the public key certificates it generates. (743)

Other security objectives within the minimum set are defined to ensure that there is adequate protection of the TTP assets (such as subscriber and TTP keys). These lead to ‘standard operating system’ security objectives for identification and authentication of TTP users, access control, and auditing of security relevant events. (744)

In addition to the ‘core’ set of security objectives for the TOE, supplementary service security objectives are defined. For example, the following security objective applies to the key recovery service: (745)

O.KEYRECOVER *The TOE must provide the means to store key material to enable future decryption of messages on behalf of the subscriber who owns the key.*

F.2.2 Security Objectives for the Environment

Security objectives for the environment are identified where there is a need for procedures to uphold the integrity of the operation of the TTP. These include: (746)

O.CERTCHECKS *Those responsible for the TTP must establish and implement appropriate procedural checks applying to:*

a) certificate generation (to ensure that the wrong data is not put into the certificate);

b) certificate verification (when needed, to ensure that subscribers are informed of the correct outcome of certificate verification).

O.INITSUBAUTH *Those responsible for the TTP must ensure that there are adequate procedures in place for authenticating subscribers and (when needed) requesting parties.*

The security objective O.CERTCHECKS is needed to ensure that the reputation of the TTP is not damaged as a result of the issuing of invalid certificates. The security objective O.INITSUBAUTH is needed so that (for example) archived private confidentiality keys (for the purposes of key recovery or key escrow) are not revealed to individuals who have no legitimate need to know. (747)

F.3 IT Security Requirements

F.3.1 Security Functional Requirements

Following the guidance described in Chapter 5, SFRs are initially selected to directly satisfy the security objectives for the TOE. For example, the security objective O.CERTMANAGE indicates a need for, *inter alia*, the capability to generate public key certificates. This SFR can be specified using FDP_DAU.2 (Data Authentication with Identity of Guarantor), as follows: (748)

CERTGEN.1 The TSF shall provide a capability to generate *public key certificates* that can be used as a guarantee of the validity of *the binding between the identified distinguished name and the identified public key, and possession of the associated private key.*

Refinement: public key certificates shall be produced in accordance with a defined standard (e.g. X.509).

The SFR CERTGEN.1 is based on FDP_DAU.2.1, with the generic term *evidence* clarified, by means of the refinement operation, substituted for the more specific *public key certificates*. A further use of the refinement operation specifies the requirement that the generated certificates shall conform to a defined standard. (749)

(Note that the PP author has chosen to use alternative labels for SFRs to those of [15408-2], since these were considered more meaningful in the context of the PP. This is permitted, but the PP author must provide a clear mapping from the SFRs to the [15408-2] functional components used.) (750)

The other element in the component, FDP_DAU.2.2, is used to specify the requirement for the capability to verify public key certificates, which is needed to satisfy the security objective O.CERTVERIFY: (751)

CERTVERIFY.1 The TSF shall provide *the TTP* with the ability to verify *public key certificates* and the identity of the *TTP* that generated the *certificate.*

Refinement: certificate verification shall involve, as a minimum:
a) signature verification;
b) checking the validity period;
c) checking for revocation.

The refinement operation is again used to change the generic term *evidence* to the specific *public key certificates*. Further use of the refinement operation introduces additional checks on the validity period of the certificate, and for revocation of the certificate. (752)

(Note that this approach is based on the guidance contained in section 6.2.6 of the Guide. Thus while individual elements have been assigned unique labels specific to the PP, all of the elements of the relevant component are included in the PP. Following the guidance of section 6.2.6, any such use of the refinement operation needs to be explained in the PP Rationale, with clear traceability to the ISO/IEC 15408 functional components and elements used to define the SFRs.) (753)

The security objective O.SIGNATURE requires the capability to generate digital signatures as proof of origin. This leads to the following SFRs, specified using FCO_NRO.1(Selective Proof of Origin): (754)

DIGITSIG.1 The TSF shall be able to generate *digital signatures* for transmitted *information* at the request of the *TTP.*

DIGITSIG.2 The TSF shall be able to relate the *identity* of the originator of the information and the *information* to which the evidence applies.

DIGITSIG.3 The TSF shall provide a capability to verify *digital signatures* to *the TTP* given [assignment: *limitations on the evidence of origin*].

Again we see use of the refinement operation, replacing generic terms with more specific terms. For example, in DIGITSIG.1 and DIGITSIG.3 (specified using FCO_NRO.1.1 and FCO_NRO.1.3, respectively), the generic *evidence of origin* is replaced by the specific *digital signatures*. In DIGITSIG.2, we see use of the refinement operation, in combination with a completed assignment, to clarify the SFR by removal of redundant wording: the word *information* is used in place of the wording '[assignment: *list of information fields*] of the information'. (755)

Having selected the initial set, the remaining SFRs are selected to satisfy ISO/IEC 15408 Part 2 dependencies or to identify other supporting functionality. For example, the following SFR is needed, in support of O.CERTMANAGE, to enable the generation of TTP keys for signature of generated certificates: (756)

TTP_KEYGEN.1 The TSF shall generate *TTP public/private key pairs* in accordance with a specified cryptographic key generation algorithm [assignment: *cryptographic key generation algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

This SFR is specified using FCS_CKM.1. For clarity, the refinement operation has been applied, substituting the generic term *cryptographic keys* with the specific *TTP public/private key pairs*. The assignments have been intentionally left uncompleted, reflecting the intended generic nature of the TTP PP. (757)

Similarly, DIGITSIG.4 is specified using FCS_COP.1 to specify the algorithms used for digital signature generation and verification, in support of DIGITSIG.1-3: (758)

DIGITSIG.4 The TSF shall perform *digital signature generation and verification* in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].

As with other worked examples, a decision needs to be made concerning the required level of audit required (i.e. *not-specified*, *minimum, basic* or *detailed).* The *not-specified* level is chosen as this provides the flexibility to identify those events that are of interest to the operation of the TTP. (759)

As noted above, the TTP PP also includes a set of functional packages defining the SFRs needed to support the secure provision of TTP supplementary services. The functional packages are clearly defined in terms of: (760)

a) the security objective to be satisfied;

b) the SFRs that are *additional* to those required for the core SFRs;

c) the core SFRs that are *modified* in support of the specified service.

For example, provision of the key recovery service (for which the security objective O.KEYRECOVER has been identified) leads to an additional SFR for key recovery. Key recovery is a form of cryptographic key access, and thus is specified using FCS_CKM.3 (Cryptographic Key Access): (761)

CM_KEYREC.1 The TSF shall perform *key recovery* in accordance with a specified cryptographic key access method [assignment: *cryptographic key access method*] that meets the following:

The specified key access method shall ensure that secret key material is protected from unauthorised disclosure and modification during distribution.

An example of a modified SFR needed for a TTP supplementary service is the modification of CERTVERIFY.1 where a certificate verification service is provided to TTP subscribers: (762)

CERTVERIFY.1 The TSF shall provide *the TTP and subscribers* with the ability to verify *public key certificates* and the identity of the *TTP* that generated the *certificate.*

Refinement: certificate verification shall involve, as a minimum:
a) signature verification;
b) checking the validity period;
c) checking for revocation.

The effect of the (minor) modification to CERTVERIFY.1 is to extend the capability to verify certificates to TTP subscribers as well as the TTP. (763)

F.3.2 Assurance Requirements

As described in Chapter 5, the assurance requirements should be derived based on consideration of the nature of the threat and the value of the assets constrained by what is technically feasible. Given that the value of the information being protected could be substantial, a relatively high level of assurance would seem to be needed. However, the constraints of technical feasibility suggest an assurance requirement of EAL4 would be appropriate. As described in [15408-3], subclause 6.2.4, page 60, EAL4 provides a moderate to high level of assurance from security engineering based on good commercial practices. It is also characterised as the highest level at which it is likely to be economically feasible to retrofit to an existing product line. (764)

F.3.3 Security Requirements on the IT Environment

For the TTP, no security requirements are placed on the IT environment: all security requirements are to be satisfied by the TOE. However, it is recognised that a compliant TOE could be based on an underlying operating system which provides the identification and authentication, access control and auditing functionality required to protect the TTP assets stored and processed by the TOE. (765)

F.4 PP Rationale

F.4.1 Security Objectives Rationale

The demonstration of the suitability of the security objectives to counter the threats may be provided by following the guidance given in Chapter 7, that is: (766)

a) showing, by means of a table, which security objectives counter which threats (e.g. T.ACERTAVAIL is addressed by O.CERTMANAGE and O.SIGNATURE), ensuring that each security objective is mapped onto at least one threat;

b) providing, for each threat, an argument as to why the identified security objectives were suitable to counter the threat.

An example of the justification of suitability is given below: (767)

T.ACERTAVAIL O.CERTMANAGE provides the means of securely generating and distributing public key certificates in a timely manner. O.SIGNATURE provides the ability to generate digital signatures in support of certificate generation.

F.4.2 Security Functional Requirements Rationale

The demonstration of the suitability of the SFRs to satisfy the security objectives for the TOE may be provided by: (768)

a) showing, by means of a table, which SFRs satisfy which security objectives (e.g. DIGITSIG.1-2 and DIGITSIG.4 address security objective O.SIGNATURE), ensuring that each SFR is mapped onto at least one security objective;

b) providing, for each security objective for the TOE, an argument as to why the identified SFRs are suitable to satisfy the security objective.

An example of the justification of suitability is given below: (769)

O.SIGNATURE DIGITSIG.1-2 and DIGITSIG.4 provide the functionality to generate digital signatures.

Since each TTP supplementary service has a corresponding security objective for the provision of that service, the rationale for each service is self-contained, and hence may be easily extracted for use in a PP or ST for TOEs that do provide the service. (770)

The demonstration of mutual support and internal consistency may be provided firstly by including a dependency analysis table, in the manner described in the guidance in Chapter 7. This may then be supplemented by an identification and discussion of the additional supportive dependencies between the identified SFRs (including, where appropriate, requirements on the underlying operating system) not highlighted in the dependency analysis. This should be constructed by considering each SFR in turn and the potential need for other SFRs to prevent it from being bypassed or tampered with. Examples include: (771)

a) TTP_KEYGEN.1 provides for the secure generation of TTP keys, and therefore supports those SFRs which rely on the use of those keys: CERTGEN.1, CERTVERIFY.1.

b) DIGITSIG.1-2&4 provide the digital signature function, and therefore support those SFRs which rely on the generation of digital signatures: CERTGEN.1.

c) DIGITSIG.2-4 provide the digital signature verification function, and therefore support those SFRs which rely on digital signature verification: CERTVERIFY.1.

F.4.3 Assurance Requirements Rationale

The construction of this part of the PP Rationale should relatively straightforward if the PP (for example) mandates EAL4 and does not specify any augmented assurance requirements. In this event it would be possible to assert that EAL4 provides a known set of mutually supportive and internally consistent assurance components, for which all assurance dependencies are satisfied. (772)

The justification for the choice of EAL may be provided along the lines described in section F.3.2 above. (773)